TRUCOS WINDOWS: CONTROLAR A DISTANCIA EL ORDENADOR

@RROBA

144

Año XII 4,95€

MC
MC EDICIONES

8 414090 201599 00144



HERRAMIENTAS PARA ASEGURAR NUESTRA INTEGRIDAD

HACK .NET
CÓMO CREAR PÁGINAS SIN VULNERABILIDADES

CREACIÓN DE BLOGS
HERRAMIENTAS PARA EL IPHONE

LA MOVILIDAD
OTRA AMENAZA PARA LA SEGURIDAD

Protege tu móvil y portátil

LA DEFENSA MÁS EFICAZ PARA LAS REDES

Y ADEMÁS...
Soluciones IPS: protección global

CRIPTOGRAFÍA
Los datos que viajan a través de la Red

RETROINFORMÁTICA
La biometría para hacer frente a amenzas



Directora: Montse Fernández
(montsef@mcediciones.com)

Colaboradores: Ferran Caldés, Toñi Herrero, Sara Rojas, Ana Rueda, Francisco Javier Palazón, Susana Velasco, Regina de Miguel, Laura Pajuelo, Jorge López.

Fotógrafos: Sebastián Romero.

Maquetación: Domingo Melero.

Publicidad
Directora comercial: Carmen Ruiz
(carmen.ruiz@mcediciones.com)
Menchu de la Peña
(mdelapena@mcediciones.com),
Orense, 11. 28020 Madrid
Tel: 91 417 04 83 . Fax: 91 417 05 33

Suscripciones: Fernando García (fgarcia@mcediciones.com)
Tel: 91 417 04 83

Edita:



Editora: Susana Cadena
Gerente: Jordi Fuertes
Redacción, Administración y Departamento de Publicidad
Paseo San Gervasio, 16-20.
08022 Barcelona
Tel: 93 254 12 50 - Fax: 93 254 12 63

Oficina de Madrid
C/ Orense, 11 bajos
2820 Madrid
Tel. 91 417 04 83
Fax: 91 417 04 84

Distribución:
Coedis S.A. Avda. de Barcelona, 225 - Molins de Rei, Barcelona
Coedis Madrid: Alcorcón,9
Pol Ind. Las Fronteras-Torrejón de Ardoz, Madrid

Fotomecánica: MC Ediciones, S.A.
Paseo San Gervasio, 16-20.
08022 Barcelona

Impresión: Rotographik

Tel. 935 747 400

Precio de este ejemplar: PVP 4,95 € (IVA incluido)
Precio para Canarias, Ceuta y Melilla:
4,95 € (incluye transporte)
Depósito legal: MA-1049-97 / nº144

¿ES "SOLO", SÓLO UN CHIVO EXPIATORIO?

Las encuestas siguen mostrando que la percepción de inseguridad retrae a muchos internautas de utilizar más intensamente el comercio electrónico. Parece pues que los contraargumentos de muchas empresas del ramo –que esgrimen que en la actualidad es más segura una transacción on line que una compra en la tienda física–, no acaban de convencer. Y es que no pasa una semana sin que se evidencie que la inseguridad on line es algo muy real. La opinión pública comprueba que se hackean desde los parquímetros hasta las webs de los políticos, pasando por las instituciones en apariencia más securizadas. Así ocurrió el pasado mes de julio, cuando nada menos que Twitter fue asaltada de nuevo por el ya famoso Hacker Croll, que en esa ocasión se hizo con la contraseña del CEO de esa red social, accediendo a más de 300 documentos sensibles, que publicó con la intención, según dijo, de demostrar que "nadie está totalmente protegido en internet".
Este clima, que se sostiene y agrava año tras año, genera una gran presión a la industria y a la administración, lo que explica en parte lo desorbitado de algunas de sus reacciones. Por ejemplo, tratando de escarmentar durísimamente a hackers sin finalidad de lucro, cuyo atrevimiento y curiosidad -y su insultante habilidad, que también juega un papel- les convierte en chivos expiatorios ideales. Éste es el caso de "Solo", Gary McKinnon, el famoso 'hacker' del Pentágono, un británico que en julio perdió su recurso para impedir su extradición a EEUU, donde podrían caerle nada menos que hasta 70 años de prisión. Su delito, que el fiscal califica de "el mayor ataque informático de la historia en el campo militar", consistió en 2001 y 2002 en acceder a 97 ordenadores de la NASA, y las fuerzas armadas norteamericanas buscando supuesta información sobre los OVNIS. Las circunstancias del caso (McKinnon está afectado por el síndrome de Arpergen, similar al autismo) hacen pensar aún más que estamos más bien ante un caso de venganza que de justicia. No se trata de felicitar a quienes infringen la ley, por supuesto, pero las administraciones mejorarían la percepción sobre seguridad si enfocaran sus energías hacia el verdadero enemigo: las bandas de delincuentes organizadas. Pero de momento, éstas siguen operando tranquilamente.

[SUMARIO número 144]





Acuerdo entre Microsoft y Yahoo!



Yahoo! y Microsoft han anunciado un acuerdo en virtud del cual a partir de ahora, la tecnología de Microsoft será la que opere las búsquedas de Yahoo!, mientras Yahoo! actuará como la fuerza de ventas exclusiva a escala mundial para los anunciantes Premium de ambas compañías.

"Este acuerdo llega cargado de valor para Yahoo!, nuestros usuarios y toda la industria. Y creo que establece las bases para una nueva era de innovación y desarrollo en Internet", afirma Carol Bartz, CEO de Yahoo!, quien añade: "Los usuarios seguirán percibiendo las búsquedas como una parte vital de su experiencia dentro de los servicios de Yahoo!, y disfrutarán de más innovación gracias a la escala y recursos que este acuerdo facilita. Los anunciantes también se beneficiarán de esta escala, contarán con una mayor facilidad de uso y disfrutarán de las eficiencias que genera trabajar con una única plataforma y un único equipo de ventas para anunciantes Premium. Por último, este acuerdo nos ayudará a aumentar nuestras inversiones en áreas prioritarias como obtener propiedades que nos hagan ganar audiencia, desplegar más capacidades en publicidad y ofrecer experiencias móviles".

Con el objetivo de ofrecer una alternativa viable para los anunciantes, este acuerdo combinará los centros de ventas de publicidad en búsquedas de Yahoo! y Microsoft, de forma que los anunciantes ya no tendrán que depender de una compañía que domina más del 70% de todo el mercado de búsquedas. Añadiendo el volumen de búsqueda de Yahoo!, Microsoft alcanzará el tamaño y escala necesarios para dar más pie a la competencia y a la innovación en este mercado, algo que beneficiará tanto para los consumidores como para los anunciantes. El CEO de Microsoft, Steve Ballmer, señala que el acuerdo proporcionará al motor de búsquedas de Microsoft, Bing, la escala necesaria para competir de forma más efectiva, atrayendo a más usuarios y anunciantes, lo que conducirá a su vez a unos resultados de búsqueda y anuncios más relevantes.

Para Juan Carlos Fernández, director general de Consumo & Online de Microsoft Ibérica, "mediante este acuerdo con Yahoo!, crearemos más innovación en búsquedas, mayor valor para los anunciantes y una capacidad de elección real para el consumidor en un mercado dominado actualmente por una sola compañía. El éxito en las búsquedas requiere tanto innovación como escala. Con nuestra nueva plataforma de búsqueda Bing, aportamos características e innovación de vanguardia. Este acuerdo con Yahoo! nos proporcionará la escala que necesitamos para llevar al mercado cada vez más rápido los últimos avances en relevancia y utilidad de las búsquedas. Microsoft y Yahoo! saben que las búsquedas online podrían ser mucho más de lo que actualmente son, y este acuerdo nos da la escala y los recursos para crear el futuro de las búsquedas".

Por su parte, Roy Bostock, presidente del Consejo de Administración de Yahoo!, indica. "Este acuerdo encaja en la dirección estratégica a largo plazo de Yahoo!, que se centra en mantenerse como la compañía de medios online líder en el mundo, y Carol Bartz cuenta con el soporte unánime de la Junta de Yahoo! en torno a este acuerdo. Se trata de una notable oportunidad para nosotros. Microsoft es un innovador dentro de la industria en las búsquedas, y es una gran oportunidad para centrar nuestras inversiones en otras áreas críticas para nuestro futuro".

Los términos del acuerdo son:

- La duración del acuerdo se ha establecido en 10 años.

- Microsoft adquirirá una licencia exclusiva de 10 años de duración sobre las tecnologías de búsqueda de Yahoo!, y Microsoft tendrá la posibilidad de integrar las tecnologías de búsqueda en sus plataformas de búsqueda por Internet ya existentes.

- Bing será el algoritmo exclusivo de búsqueda y la plataforma de búsquedas pagadas para los sitios de Yahoo!. Yahoo! continuará usando su tecnología y sus datos en otras áreas de su negocio como en las pantallas destacadas y en la tecnología de búsqueda.

- Yahoo! será la fuerza de ventas exclusiva para los anunciantes Premium en las búsquedas. La publicidad autocontratada en ambas compañías se servirá a través de la plataforma AdCenter de Microsoft, y los precios para toda la publicidad en búsquedas se seguirán colocando por el proceso de subasta automática de AdCenter.

- Cada compañía mantendrá su propio negocio de publicidad en display y su propia fuerza de ventas.

- Yahoo! innovará y seguirá siendo el propietario de la experiencia de usuario en sus dominios, incluyendo la experiencia de búsquedas, incluso si está basada en la tecnología de Microsoft.

- Microsoft compensará a Yahoo! a través de un trato de compartir ingresos del tráfico generado en la red de Yahoo!, en sitios propios y gestionados (O&O), así como en lugares afiliados.

- Microsoft pagará los costes de adquisición de tráfico (TAC) a Yahoo! a una tarifa inicial del 88% de los ingresos generados en los sitios O&O de Yahoo! durante los primeros cinco años del acuerdo.

- Yahoo! continuará sindicando sus colaboraciones en búsquedas afiliadas.

- Microsoft garantizará los ingresos de Yahoo! en sus sitios por búsquedas (RPS) en cada país durante los primeros 18 meses de implementación inicial en cada país.

- Hasta que se llegue a la implementación plena (se espera que suceda en los 24 meses siguientes a la aprobación por el organismo regulador), Yahoo! estima en función de los niveles de ingresos actuales y a los gastos de operador, que este acuerdo generará un beneficio anual de aproximadamente 500 millones de dólares y unos ahorros de aproximadamente 200 millones. Yahoo! también considera que este acuerdo proporcionará un beneficio en el flujo de caja operativo de aproximadamente 275 millones de dólares.

- Este acuerdo protegerá la privacidad del consumidor limitando los datos compartidos entre las dos compañías a los mínimos necesarios para operar y mejorar la plataforma de búsqueda combinada, y restringirá el uso de los datos de búsquedas compartidos entre las dos compañías. El acuerdo mantiene las prácticas de privacidad que ambas compañías siguen hoy.

- El acuerdo no cubre las propiedades y productos de cada compañía, correo electrónico, mensajería instantánea, publicidad en display u otros aspectos de los negocios de las compañías. En esas áreas, ambas compañías seguirán siendo competencia como hasta ahora.

La transacción estará sujeta a una revisión por parte del organismo regulador. El acuerdo concretado anticipa que las partes entrarán en unos acuerdos más detallados antes de que se cierren todos los puntos. Microsoft y Yahoo! esperan que este acuerdo se revise atentamente por parte de los reguladores de la industria y del gobierno y agradecen cualquier tipo de pregunta. Las compañías esperan que se pueda cerrar a principios del año 2010.

Mueve un dedo por los Derechos Humanos

Amnistía Internacional lanza una nueva línea de Artículos Digitales para que conviertas tu ordenador en un símbolo de denuncia. Esta nueva línea de "Artículos Digitales" de Amnistía Internacional promueve el activismo por los derechos humanos desde cualquier ordenador, con un simple ¡clic!



Con esta original iniciativa, Amnistía Internacional inaugura una nueva forma de reivindicar los derechos humanos a través de su tienda on line www.actuaconamnistia.org/tienda donde están disponibles para su descarga "Los Protestones", muñecos recortables que protestan contra la censura, la pena de muerte y la discriminación de las minoría sexuales, y "Los Salvapantallas por los Derechos Humanos", una recopilación de clips de video arte entorno a la Declaración Universal de Derechos Humanos. Todos ellos a un precio de sólo 1 euro. Este microdonativo es útil para que Amnistía Internacional, que no solicita subvenciones ni recibe fondos de ningún gobierno nacional, pueda continuar con su lucha a favor de los derechos humanos, manteniendo su independencia.

Ya están disponibles en la tienda on line de Amnistía Internacional los 12 primeros artículos de la Declaración. Periódicamente la organización incluirá nuevas creaciones. La igualdad ante la ley, la abolición de los malos tratos y la tortura, el derecho a la vida o la libertad de expresión son derechos humanos irrenunciables que aparecerán en tu pantalla para que tu ratón nunca permanezca inmóvil frente a las injusticias.

"Los productos quieren acompañar a los cibernautas donde más tiempo pasan: delante del ordenador, bien en la pantalla o junto al teclado. Nuestro objetivo es que todas las personas, y en todo momento, hasta realizando sus tareas cotidianas, pueda aportar su granito de arena en nuestra lucha por defender los derechos humanos", asegura Marcos Macarro, portavoz de Amnistía Internacional. Todos los productos se presentan bajo el sello Creative Commons que permite su libre difusión siempre que se produzca con un fin no comercial.



Organizados como empresas para atentar en la Red

A medida que avanza 2009, los ataques en la Red son más sofisticados y los delincuentes informáticos operan cada vez más como si de grandes empresas se trataran, copiando algunas de sus mejores estrategias y colaborando unos con otros para que sus actividades ilegales sean más lucrativas. Así los cibercriminales utilizan SaaS, motores de búsqueda y otras estrategias para perpetrar sus ataques. Éstas son algunas de las conclusiones que revela el último estudio sobre seguridad en la Red que ha llevado a cabo Cisco. En el informe también se destacan algunas de las estrategias y técnicas más habituales que los delincuentes aplican para abrir brechas de seguridad en las redes corporativas. Poner en peligro los sitios web de las empresas o robar información personal y dinero, suelen ser algunas de las prácticas habituales de estos cibercriminales. Para estar protegidos contra algunos de los nuevos tipos de ataque, Cisco incluye en el informe algunas recomendaciones que tienen en cuenta a personas, procesos y tecnologías, desde un enfoque global para la gestión de los riesgos.

Los delincuentes informáticos han empezado a colaborar entre ellos y se aprovechan de los temores e intereses de los individuos, haciendo cada vez mayor uso de las herramientas legales de Internet, como motores de búsqueda y el modelo de software como servicio (SaaS). En lo que llevamos de 2009, los ataques más sofisticados han sido protagonizados por Conficker y epidemias como la Gripe A.

B2B Suite 6.0, para simplificar los complejos entornos de transacciones

iWay Software, división de Information Builders de soluciones de gestión de información empresarial, ha anunciado el lanzamiento de iWay Software B2B Suite 6.0, un producto ampliado que permite mantener de forma rápida y sencilla acuerdos con partners y desplegar relaciones comerciales a través de protocolos estándar de Internet. Con un interface avanzado e intuitivo, y la interoperabilidad y extensibilidad que brindan los productos de business intelligence (BI) e integración de Information Builders, la suite Business-to-Business (B2B) de iWay Software permite a las empresas gestionar las comunicaciones B2B con múltiples partners utilizando cualquier número de series de mensajes y protocolos diferentes. Uno de los componentes clave de iWay B2B Suite es iWay Trading Partner Manager, que gestiona la información y la infraestructura de los socios comerciales haciendo de las interacciones B2B una extensión natural de la integración de aplicaciones en cualquier organización.



Más productividad y eficiencia del servicio virtual de atención al cliente

La nueva aplicación one-X Agent de Avaya, aplicación de escritorio diseñada para asociados de servicios de atención al cliente, ofrece mejoras que incluyen una racionalizada interfaz para el usuario con vídeo incorporado y opciones de despliegue aumentadas, que puede mejorar la productividad y el costo/eficiencia en las, cada vez más frecuentes, operaciones virtuales de servicio al cliente. Asimismo, permitirá a los asociados trabajar de forma más flexible. Las nuevas mejoras que llevan a una mayor productividad incluyen una interfaz de usuario que permite a los asociados de atención al cliente manejar múltiples interacciones del cliente de forma simultánea. Esto ayuda a simplificar la gestión del trabajo para el usuario y tiene como resultado una mayor resolución en la primera llamada del proceso de atención al cliente. La interfaz de usuario también presenta nuevas herramientas tales como una lista de contactos integrada con un 'clic y marcar' y 'arrastrar y soltar' para transferencias y conferencias, otorgando a los asociados de atención al cliente más efectividad a la hora de llegar al experto adecuado e incluirlo en las interacciones con el cliente.



Aumenta el malware transmitido por email y se retarda su detección

Los principales motores antivirus tardan en detectarlo entre 4 y 80 horas, según revela Cyberoam en un estudio sobre las tendencias de amenazas en Internet correspondiente al segundo trimestre de 2009. Elaborado en colaboración con Commtouch, el informe pone de manifiesto el incremento significativo del número de virus nuevos que circulan a través del correo electrónico y frente a los que los principales motores antivirus han sido incapaces de defenderse, dejando las redes desprotegidas durante varias horas.

Los atacantes siguen buscando medios creativos para sortear las soluciones de seguridad. Un ejemplo de ello es una nueva variante de "phishing" (suplantación de identidad), que se vale de un método único de redirección que les permite sortear las soluciones tradicionales de filtro de URL, ocultando el código entre páginas alojadas en un sitio educativo legítimo que han usurpado previamente. Otra tendencia que ha resurgido es la de los mensajes spam de imágenes, (ahora se utilizan tácticas nuevas, tales como estándares anteriores en formato MIME para sortear los filtros de spam tradicionales, así como los filtros de Gmail). Por otro lado las estafas más fraudulentas, como el 419 nigeriano, siguen generando titulares.

Entre otras amenazas de este trimestre se encuentra la utilización de acontecimientos de actualidad para apelar a las emociones de los destinatarios. Sucesos mundiales, como la muerte de la superestrella del pop Michael Jackson y la propagación de la fiebre porcina, han sido objeto de nuevo spam. En las tendencias de Web 2.0, el streaming media y las descargas se encuentran también son dos de las más populares dentro de la categoría de sitios con contenido generado por usuarios.

¿A quién te gustaría que avisaran los servicios de emergencia si te pasara algo?

El Ministerio del Interior y Cruz Roja Española han lanzado la campaña "Aa" (Avisar a...) con el objetivo de que los usuarios de teléfono móvil incluyan en su agenda el contacto Aa, seguido del nombre de la persona con la que habría que ponerse en contacto en caso de emergencia. Así, ese número de teléfono aparecerá siempre como el primer contacto de la lista.

El contacto Aa permitirá a los servicios de emergencia y los cuerpos de seguridad contactar de forma rápida con el entorno de las víctimas de accidentes, personas que se encuentran en situaciones de urgencia o sin posibilidad de comunicarse.



Guía de navegación segura de PandaLabs

Aunque el verano es una época para relajarse y estar tranquilo, hay un aspecto en el que no se puede bajar la guardia: la seguridad informática. Y es que los ciberdelincuentes no se van de vacaciones. La época veraniega es propicia para hacer un uso del ordenador más lúdico que en el resto de año. El uso de servicios como chats, juegos online, descargas de software o compras online, se disparan durante esos períodos debido a que muchos usuarios disponen de más tiempo libre. Además, los más pequeños de la familia están disfrutando de sus vacaciones y pasan más horas delante del ordenador.

Los delincuentes de Internet también son conscientes de ello y, por tanto, están siempre al acecho para tratar de conseguir nuevas víctimas. Por esa razón, PandaLabs nos ofrece una guía de navegación para asegurarse de que el ordenador está bien protegido este verano:

- Prestar especial atención al correo electrónico, ya que es una vía tanto de entrada de amenazas, como de ataques de phishing o timos en forma de spam.

- Instalar sin demora las últimas actualizaciones de seguridad. Con mucha frecuencia los ciberdelincuentes utilizan agujeros de seguridad en programas de uso común para llevar a cabo sus ataques.

- Tener cuidado con la información que da en las redes sociales. Así se recomienda no hacer público, por ejemplo, el día que se comienzan las vacaciones y menos aún si en esa misma red social hay datos sobre el lugar de residencia.

- Evitar la descarga de programas desde lugares no seguros en Internet, ya que pueden estar infectados.

- Dejar el router apagado. De esta manera, se evita que se produzcan conexiones ajenas a la red del usuario.

- Ser precavido si usan ordenadores compartidos en cibercafés o locutorios, por ejemplo. En esos casos se recomienda no activar la opción que permite guardar en el equipo las claves que se teclean, cuando se introduzca el nombre de usuario y contraseñas en ordenadores públicos. Igualmente se ha de evitar utilizar ordenadores compartidos para realizar transacciones bancarias.

- Utilizar programas con Control Parental, una herramienta que ayuda a determinar qué páginas pueden ver sus hijos y cuáles no, a qué información pueden acceder o no, etc.

- Asegurarse de que el ordenador cuenta con una solución de seguridad activa y actualizada en todo momento. Hay programas antivirus gratuitos como el nuevo Panda Cloud Antivirus que pueden descargarse desde www.cloudantivirus.com



Detectadas casi 600 nuevas variantes de Koobface

Kaspersky Lab ha registrado una explosión de variantes de Koobface durante el mes de junio, motivada por la llegada del verano y el período vacacional. Tan sólo en un mes, el número de variantes detectadas ha pasado de 324 a finales de mayo a casi 1.000 a finales de junio de 2009. El gusano Koobface fue detectado por primera vez por los analistas de Kaspersky Lab como Net-Worm.Win32. Koobface y saltó a la fama hace poco menos de un año cuando empezó a atacar cuentas de Facebook y MySpace. Koobface se propaga a través de la cuenta legítima de un usuario a los perfiles de sus amigos. Los comentarios y mensajes enviados por el gusano contienen un link a un sitio falso de YouTube que invita a los usuarios a descargarse una "nueva versión de Flash Player". El gusano, en lugar de instalar el programa, se descarga en los ordenadores de las víctimas. Una vez que un usuario ha sido infectado su PC comienza a enviar el mensaje a sus contactos, mientras la funcionalidad del gusano se sigue extendiendo. Koobface se sigue centrando en la actualidad en atacar más sitios de redes sociales como Facebook, MySpace, Hi5, Bebo, Tagged, Netlog y, más recientemente, Twitter. A medida que estas redes sociales ganan popularidad, son cada vez más frecuentes los ataques que se dirigen a ellas.

Net-Worm.Win32.Koobface
Nuevas versiones identificadas por Kaspersky Lab

per day — total

Recomendaciones de Kaspersky Lab:

-ser cauteloso a la hora de abrir enlaces que llegan a través de mensajes sospechosos. Incluso si el remitente es un amigo.

- Utilizar Internet Explorer 7 o Firefox en modo seguro e instala la opción HYPERLINK "http://noscript.net/"NoScript.

- Revelar la menor cantidad de información personal que sea posible. No publicar la dirección, teléfono u otros detalles privados.

-Mantener el software antivirus actualizado para prevenir que las nuevas versiones de malware ataquen al ordenador.



Microsoft celebra el 10º Aniversario de Windows Live Messenger



La decimotercera edición de la Campus Party ha coincidido con el décimo aniversario de Windows Live Messenger, que Microsoft celebrará con los "campuseros". Microsoft Ibérica, patrocinador una vez más del evento, contó con dos dispositivos Surface para los que se desarrolló una aplicación que permitió a los visitantes crear temas personalizados de una forma muy sencilla e intuitiva con motivos de Messenger, como emoticonos o buddies. Al terminar su diseño, los creadores elegían si se lo envían por correo electrónico como fondo de escritorio o lo imprimía en el momento en un vinilo que podrán pegar en su PC.

Además durante el evento, la compañía presentó su Marketplace, un lugar donde los usuarios pueden buscar, navegar y comprar aplicaciones móviles desde un teléfono Windows o desde un PC, usando simplemente una identidad Windows Live ID. También los "campuseros" pudieron participar de la iniciativa Imagine Mobile, que promueve la creación de innovadoras aplicaciones para los teléfonos Windows, que enriquecerán la nueva tienda online Marketplace y crearán nuevas experiencias para los usuarios. Las tres mejores propuestas de Campus Party se llevaron un teléfono Windows. Además la Campus Party ha sido el escenario de la presentación, por primera vez al gran público en España, de Windows 7.

Nuevo centro de datos de Arsys

Este nuevo centro de datos está ubicado en las inmediaciones de Logroño (La Rioja). La actual sede y las oficinas administrativas y de servicios corporativos se mantendrán en el centro de Logroño.

Diseñado sobre un pabellón empresarial ya existente, el nuevo centro de datos ocupa una superficie total de 6.000 m2. Esta superficie se distribuye entre espacio para los servidores (salas técnicas), sistemas de disponibilidad (alimentación, climatización, conectividad, seguridad lógica, monitorización...) y logística (almacenaje, envío y recepción de mercancía...). Aproximadamente unos 300 m2 se destinan a oficinas, ya que 40 personas del equipo técnico de Arsys tienen su nuevo centro de trabajo en estas instalaciones.

El suelo técnico disponible para servidores alcanza los 1.000 m2, distribuidos en cuatro salas técnicas e independientes de 250 m2 cada una. Estas dimensiones permitirán el alojamiento de 15.000 servidores, multiplicando por cinco la capacidad de los dos centros de datos que opera actualmente la empresa.

Las obras de adecuación del edificio comenzaron en marzo de 2009, tras un trabajo previo para el estudio de las necesidades de la compañía. En julio, sólo cuatro meses después, el centro de datos está preparado para recibir los primeros servidores. El traslado de las máquinas desde las instalaciones que tenía Arsys antes de la construcción de este centro de datos se realizará progresivamente. Este centro de datos garantiza la eficiencia y los niveles de servicio que la compañía presta a sus clientes. También facilitará el crecimiento de la empresa durante la próxima década, al permitir el suministro de servicios de Internet con unos niveles de disponibilidad muy elevados y altamente competitivos, gracias al control de aspectos críticos, como el consumo energético.

España, uno de los paraísos preferidos por los spammers

Los spammers se aprovechan de estas épocas del año, al igual que sucede en Navidad, donde los usuarios consumen más a través de Internet, ya sea para realizar compras espontáneas o bien una reserva de viaje. De esta manera, los piratas informáticos se hacen con la confianza del usuario, siendo éste totalmente vulnerable ante sus habilidades, para convertirlo finalmente en un blanco fácil de sus ataques.

Por ello que SPAMfighter avisa a todos los usuarios que tengan cuidado al abrir y leer e-mail, o al adquirir productos a través de correos de dudosa procedencia, ya que los ataques son varios y cada vez más sofisticados y con contenidos dedicados a distintos países.

En estas épocas del año donde es muy común que los usuarios feliciten a sus conocidos las vacaciones de verano o bien las de Navidad vía e-mail, y cuando el usuario hace clic en los links para obtenerlos el ordenador se ve infectado por un código malicioso.

En palabras de Martin Thorborg, cofundador de SPAMfighter, "los spammers saben que durante el verano mucha gente felicita las vacaciones a amigos y parientes a través del correo electrónico. Es aquí cuando los piratas informáticos entran en acción y se aprovechan de la situación; los usuarios abren estos correos de felicitación que son falsos y se convierten fácilmente en víctimas de estos ciberladrones".

Debido a ello, SPAMfighter recomienda lo siguiente:

- No hacer compras Online a través de un correo electrónico de dudosa procedencia, aunque se trate de una excelente oferta.
- Crear una cuenta de correo gratuita para las compras Online y así evitar posibles amenazas. Realizar un seguimiento de dichas compras Online.
- Antes de hacer compras online, descargar o actualizar el filtro anti-spam para estar protegido.

Una de las cuestiones que permiten estos engaños es la confianza que tienen los usuarios. Debido a ello, SPAMfighter, que protege a todos sus usuarios y bloquea más del 90% de ataques phishing junto con el spam tradicional, filtra automáticamente los e-mails no deseados de la bandeja de entrada de todos sus usuarios, velando por su seguridad, ya que los firewalls tradicionales y los programas antivirus, no detectan este tipo de amenazas.

Nuevos Servidores Premium de 1&1

1&1 Internet España ha presentado sus nuevos Servidores Dedicados Premium. Desde ese momento, los clientes de 1&1 pueden elegir entre 8 diferentas configuraciones de Hardware para los Servidores Dedicados Linux, Windows y los Servidores Gestionados. Todos ellos incluyen en su precio transferencia ilimitada de datos. Además, todos los servidores cuentan con 250 GB de espacio de backup mediante FTP.

En 1&1, los clientes pueden elegir entre cinco Servidores Dedicados con procesadores Dual-Core y tres opciones con procesadores Quad-Core. Las nuevas propuestas son el Dual-Core S, Dual-Core M y Dual-Core XXL. El modelo básico de los Servidores Dedicados de 1&1, el Dual-Core S, está disponible por el económico precio de 39,99 euros/mes (49,99 euros versión Windows) con procesador AMD Athlon 3800+ y 2 discos duros de 160 GB con tecnología Raid 1.

El Servidor Dual-Core M ofrece, por tan solo 49,99 euros al mes (59,99 euros versión Windows) un procesador AMD Athlon 4200+, con 2 x 2,2 GHz, tecnología Raid 1, 2 discos duros de 250 GB y 2 GB de memoria RAM. Con el Servidor Dual-Core XXL, el usuario puede beneficiarse de 2 procesadores Opteron 2216 HE y 8 GB de memoria RAM. Durante junio hay una oferta por la que durante los primeros seis meses, el Servidor Dedicado Dual-Core XXL de 1&1 estará disponible por tan solo 69,99 euros al mes, a partir del séptimo mes su precio mensual será de 149,99 euros (para Windows 79,99 euros/mes y 169,99 euros/mes respectivamente). Los usuarios profesionales reciben con el Servidor Quad-Core XXL Premium de 1&1 un auténtico sistema Raid 5 con tres discos duros y 1.500 GB útiles de disco duro, y gracias a los dos procesadores AMD Opteron 2352 se obtiene el rendimiento total de ocho núcleos. Contiene además un total de 16 GB de RAM. El servidor high-end de 1&1 estará disponible por poco tiempo a 149,99 euros/mes durante seis meses y luego a 299,99 euros/mes (para Windows 159,99 euros/mes y 319,99 euros/mes respectivamente).

Core Protection para máquinas virtuales

Con este lanzamiento, Trend Micro amplía su portfolio de seguridad en materia de virtualización con la incorporación de una solución de seguridad de contenidos para proteger los entornos VMware ESX/ESXi. Trend Micro Core Protection for Virtual Machines ha sido diseñada para asegurar las máquinas virtuales VMware, tanto de las amenazas que están activas como de las inactivas, de forma completa y con efectividad.

El producto utiliza las APIs VMsafe de VMware para ofrecer protección estratificada empleando un escaneo dedicado de VM y coordinado en tiempo real con los agentes dentro de VM. Mientras que la virtualización de servidores incrementa la eficiencia en los centros de datos, también crecen los retos de la seguridad en el entorno TI: las soluciones de seguridad de contenidos existentes importadas desde el mundo físico habitualmente dejan brechas de seguridad cuando se despliegan en entornos virtuales.

Por ejemplo, las máquinas virtuales que están inactivas o que están desconectadas pueden llegar a infectarse incluso cuando no están siendo utilizadas y todavía no son capaces de protegerse con un agente de escáner antivirus y actualizaciones de firmas.

De forma parecida, las operaciones de seguridad que emplean muchos recursos como el escaneo de sistemas completo programado pueden reducir significativamente el rendimiento del host y dar lugar a una seguridad inefectiva, especialmente cuando se realiza de forma simultánea en varios equipos virtuales. El nuevo Trend Micro Core Protection for Virtual Machines está optimizado para virtualización y cierra las brechas de seguridad en entornos virtualizados.

Protege las máquinas virtuales activas e inactivas, proporcionando escaneo y actualización de patrones desde un equipo virtual de escaneo independiente, y mejora el rendimiento de los servidores virtuales. Asimismo proporciona protección malware de primera calidad, asegurándose de que las máquinas virtuales están protegidas incluso cuando están inactivas y preparadas para las últimas actualizaciones de patrones cuando sean activadas.

¿Cuánto valoras tu vida digital?

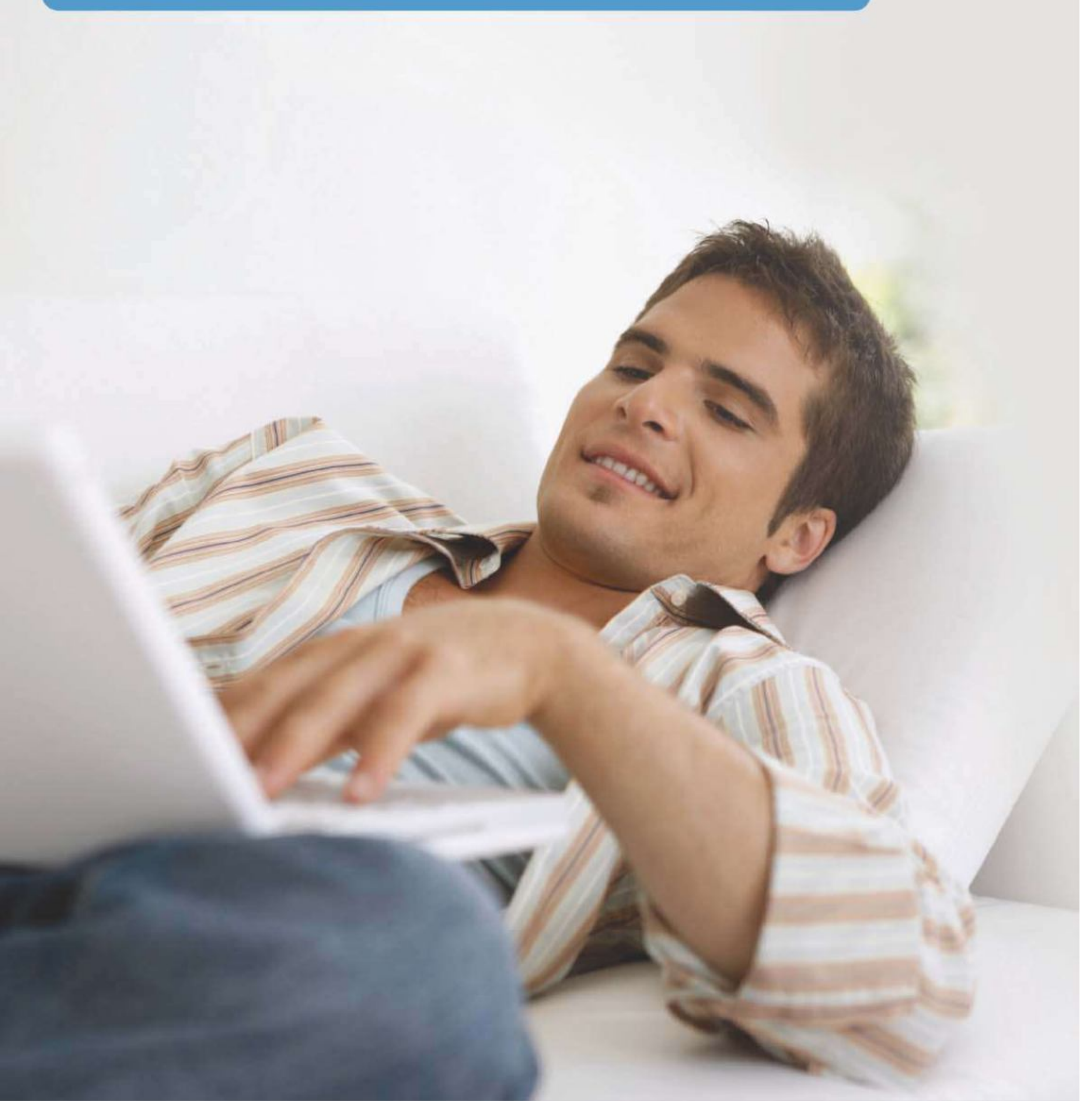
Un nuevo estudio realizado por Symantec se hace eco del uso cada vez más extendido del ordenador para "almacenar de por vida" sus contenidos digitales. De ahí la fuerte conexión emocional existente con la amplia gama de archivos importantes que los usuarios almacenan en los PC, produciéndose así en éstos rabia, dolor y angustia ante la potencial pérdida digital de sus valiosos datos digitales. Un hecho, por otra parte, más común de lo que imaginamos, ya que un 44% de las personas encuestadas ha perdido datos de mucho valor emocional. Las fotografías, según esta encuesta, se sitúan en primer puesto en cuanto al impacto emocional que supondría su pérdida en los usuarios, seguidas de la información financiera y documentos académicos o de trabajo. Pero, a pesar de ello, sólo el 22% de los encuestados realiza una copia de seguridad de todos sus archivos. De los 3.000 encuestados, el 77% afirma haber realizado copias de seguridad de alguno de sus archivos pero, utilizando para ello métodos como hardware externo o discos. Y tan sólo un 11% de los encuestados indicó utilizar almacenamiento online seguro a la hora de realizar copias de seguridad. Por ello Symantec propone su solución para copias de seguridad Norton Online Backup, que ha sido diseñado para simplificar la realización de copias de seguridad de sus fotografías digitales, documentos financieros esenciales, colecciones de música y correo electrónico archivado, y todo ello utilizando un sitio web fácil de usar.



El único hosting...
con tranquilidad de serie

Tranquilidad para ti y para tus clientes. Porque arsys.es te ofrece toda la calidad, seguridad e innovación que necesitas para tus proyectos online. Con servicios integrales de alojamiento y **las soluciones hosting más avanzadas del mercado**: desde el más fiable VPS al pionero Cloud Hosting. Respaldados siempre por las mejores marcas y con **Soporte Total 24/7**. Y todo ello, además, en tu propio idioma.

Disfruta de las ventajas y garantías de una marca líder, ¡y trabaja tranquilo!





VPS



Control y libertad

La **solución eficiente y económica** para aquellos que necesitan libertad en la administración de su propio servidor y en la instalación de aplicaciones. Además con disponibilidad inmediata y **garantía de reembolso de 30 días**.



Cloud Flexible



Flexibilidad. Potencia. Estabilidad. Ahorro.

Una nueva solución flexible y escalable que crece según lo hacen tus proyectos. Configura sólo los recursos que necesites: CPU, memoria, disco duro y transferencia. Además, **sólo se te factura por lo que quieras utilizar.**



Dedicados



Potencia e independencia

Para proyectos que implican total dedicación y gran disponibilidad de recursos, arsys.es te ofrece las mejores marcas (**IBM**), garantía ilimitada del hardware y el **máximo rendimiento** y seguridad.



Soluciones a tu medida

arsys.es dispone de la capacidad técnica y humana para ofrecer **soluciones avanzadas de alojamiento dedicado bajo demanda**. Sean cuales sean los requerimientos de tu proyecto, tenemos la solución: servidores a medida, balanceo de carga y almacenamiento masivo.

La tecnología Wi-Fi permite a un gran número de equipos conectarse al mismo tiempo a la Red de manera inalámbrica. Pero, ¿hasta que punto es esto seguro? Existen varios métodos para evitar que otras personas no autorizadas accedan al punto de acceso o intenten incluso hacerse con los datos privados.

Conectividad Wi-Fi ¿es segura?





>>> TRES MOTIVOS POR LOS QUE DESECHAR WEP

La mayoría de las redes domésticas y de las oficinas utilizan WEP para protegerse de los ataques. Pero mucha gente no sabe los peligros que esto acarrea. Y es que este protocolo de seguridad puede ser inútil ante varios ataques diseñados por los hackers que les permiten infiltrarse en redes WEP. Principalmente podemos hablar de tres:

• Ataque de diccionario: Algunos usuarios conservan ajustes de fábrica en sus puntos de acceso inalámbrico y en sus tarjetas de red inalámbrica. Otros, escogen claves débiles que pueden averiguarse fácilmente en un diccionario idiomático. Ambos están a merced de los hackers, que a través de algoritmos sofisticados pueden "adivinar" la clave. Es quizás el más evitable ya que basta con elegir una contraseña complicada.

• Ataque de intermediario: Muchos de los routers emiten su SSID para que los clientes encuentren su señal rápidamente y puedan conectarse de manera fácil. Un router corrupto puede engañar fácilmente al usuario para que éste le envíe su información de seguridad, proporcionando al hacker la información que requiera para acceder a la Red verdadera. Para solucionarlo, ayuda desactivar el broadcasting SSID.

• Ataque de repetición: Se produce cuando un pirata informático intercepta paquetes de comunicación inalámbrica y graba la información transmitida. De este modo, utiliza los datos para retransmitir mensajes con datos falsos y erróneos que pueden engañar al punto de acceso para que transmita paquetes de protocolo de resolución de direcciones. En ellos hay información suficiente para que el hacker pueda decodificar la clave WEP.

La tecnología Wi-Fi se extiende a una gran velocidad en los hogares españoles. Según el "Informe Wi-Fi 2008", elaborado por el Observatorio Wireless del Grupo Gowex, en nuestro país hay ya más de once millones de usuarios de redes inalámbricas. Sobre sus ventajas mucho se ha hablado, pero, ¿qué hay de los nuevos peligros que lleva implícitos esta tecnología? El principal de ellos se relaciona con al seguridad. En especial si la instalación permanece abierta. En este caso, cualquier ordenador que se encuentre cercano al punto de acceso puede conectarse a Internet a través de él (siempre y cuando tenga tarjeta Wi-Fi integrada, claro). Y lo que es aun más preocupante: un usuario con conocimientos avanzados podría utilizar esta conexión para acceder a la red interna o al equipo particular, analizando toda la información de la que se dispone, incluidas contraseñas, cuentas de correo, conversaciones por MSN, etcétera.

Un poco de historia

Nokia y Symbol Technologies crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica). Esta asociación pasó a denominarse Wi-Fi Alliance en 2003 . El objetivo de la misma fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma en abril de 2000 WECA certifica la interoperatibilidad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.

En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

Algunos parámetros de conexión

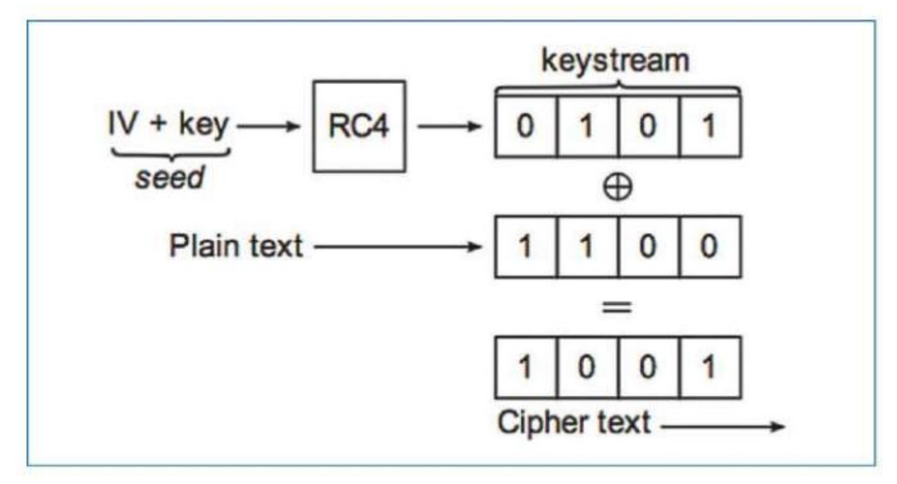
Cuando un usuario adquiere un router wireless conviene que conozca algunos de los parámetros que debe controlar:

· **El identificador SSID:** Es el nombre de la red Wi-Fi que crea el punto de acceso. Suele venir por defecto con el nombre del fabricante, si bien es posible cambiarlo y poner el que se desee.



http://www.wi-fi.org/

PESE A QUE SUS DEBILIDADES SE HAN DEMOSTRADO DURANTE LOS ÚLTIMOS AÑOS, AUN MUCHOS FABRICANTES LANZAN SUS ROUTERS WI-FI CONFIGURADOS POR DEFECTO CON ENCRIPTACIÓN WEP. ES POR ELLO TODAVÍA UN SISTEMA QUE TIENE VIGENCIA Y QUE SIGUE SIENDO EL MÁS UTILIZADO POR ENCIMA INCLUSO DE WPA.

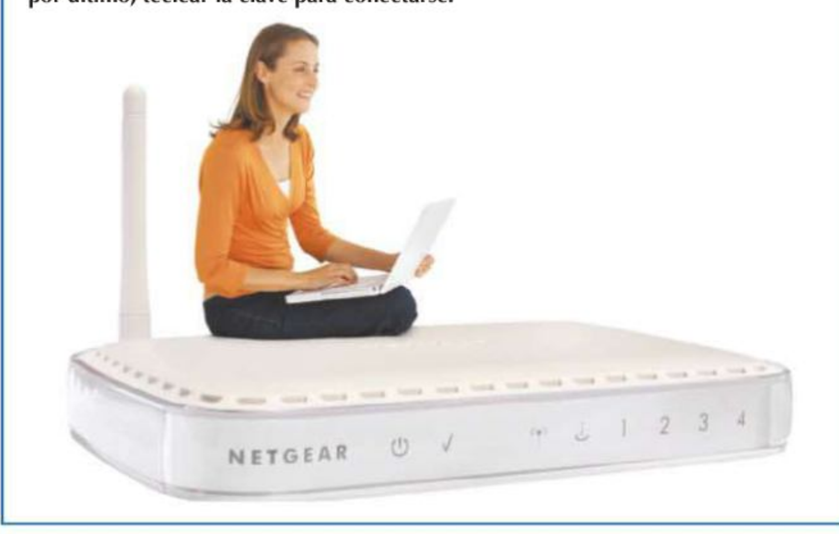


Wep crypt alt

>>> ¿CÓMO MONTAR UNA RED CERRADA WPA?

WPA es el medio más seguro para evitar que existan intrusiones indeseadas en una Red privada. Para hacerlo es necesario configurar por un lado el router o punto de acceso, y por otro, los ordenadores que vayan a conectarse al mismo. Empezaremos por el primero. Lo primero que se debe hacer es abrir el menú de configuración escribiendo en la barra de navegación del ordenador la dirección 192.168.1.1. Para entrar a ella será necesario introducir una contraseña que viene incluida en el manual de uso del router. Una vez dentro debe buscarse un menú llamado Security o Network Authentication, seleccionando en él la opción WPA, e introduciendo finalmente la clave para acceder a la red Wi-Fi.

El segundo paso es configurar los distintos equipos conectados. Utilizando como referencia el sistema Windows XP o Vista, hay que acceder al icono de conexión a redes inalámbricas. Aparecerá en la pantalla una lista de las redes disponibles indicando cuales están cerradas y cuales abiertas. Basta con seleccionar la que se desea, en la ventana siguiente señalar que se va a emplear seguridad WPA-TKIP, y, por último, teclear la clave para conectarse.



- **El canal:** Normalmente viene prefijado el canal 6 si bien puede elegirse uno cualquier entre el 1 y el 11.
- **La clave WEP (Wired Equivalent Privacy):** Es la que se encarga de encriptar la red. Al introducirla, los ordenadores que se encuentren en el entorno con capacidad Wi-Fi podrán acceder a la Red.
- **La clave compartida WPA (Wi-Fi Protected Acces):** Parecida a la anterior pero posterior y bastante más segura.
- **Cifrado de 128 bits:** Tanto en WEP como en WPA las comunicaciones se deben transmitir cifradas de tal manera que queden bien protegidas. Cuanto mayor sea el cifrado más complicado resultará romper la clave.

WEP

Pese a que sus debilidades se han demostrado durante los últimos años, aun muchos fabricantes lanzan sus routers Wi-Fi configurados por defecto con encriptación WEP. Es por ello todavía un sistema que tiene vigencia y que sigue siendo el más utilizado por encima incluso de WPA. Para su funcionamiento usa el algoritmo de cifrado RC4, que trabaja expandiendo una semilla ("seed" en inglés) que origina una secuencia de números pseudoaleatorios de tamaño mayor. Esta secuencia de números se unifica con el mensaje mediante una operación XOR, permitiendo lograr un mensaje cifrado que puede ser de 64 bits o de 128 bits.

Los inconvenientes con los que cuenta son varios. Ya de por sí el sistema no es del todo fiable: al no implementar adecuadamente el vector de iniciación del algoritmo RC4, ya que utiliza un enfoque directo y predecible para incrementar el vector de un paquete a otro, resulta fácilmente vulnerable para hackers. Asimismo, en lo que se refiere a las claves establecidas por los ISP, resultan sencillas de descubrir. Supuestamente se entrega a cada equipo una clave aleatoria singular de trece caracteres que permite al usuario autentificarse ante el router y poder acceder a la Red.

Pero la realidad es que no es del todo aleatoria: el primer número corresponde al fabricante, los seis siguientes, a los seis primeros caracteres de la dirección MAC (Media Acceso Control), y el nombre de



>>> ASUNTOS PRIVADOS EN LUGARES PÚBLICOS

Es cada vez más habitual que los usuarios de ordenadores portátiles vayan a cafeterías u otros lugares públicos a conectarse a Internet. También es normal acudir a locutorios u otros establecimientos a utilizar los servicios de un equipo público. Pese a que, por lo general, se trata de redes seguras, conviene tomar una serie de precauciones ya que de lo contrario, los datos privados pueden correr el riesgo de estar expuestos a hackers:

EN EL CASO DE USAR UN ORDENADOR PÚBLICO:

No señalar nunca la opción de guardar nombre de usuario o contraseña al acceder al correo o a alguna red social.

A ser posible, no introducir números de cuenta o datos bancarios, ya que si el equipo tiene algún tipo e virus o troyano, se puede ser víctima de robo de cuentas on-line.

Para solucionar estos dos aspectos, puede ser interesante buscar si el navegador incluye la opción de navegación privada, que hará que no quede ningún rastro en el ordenador.

EN EL CASO E UTILIZAR UN ORIENTADOR PERSONAL EN UN LUGAR CON CONECTIVIDAD WI-FI:

Se antoja necesario contar con un Firewall potente que no permita a otros usuarios acceder a las carpetas o al equipo.

Para no sufrir intrusiones indeseadas cuando no se utilice Internet en un lugar de este tipo, es preferible apagar la señal Wi-Fi.

Proteger las carpetas de herramientas es otra de las prioridades. Para ello, lo mejor es utilizar herramientas de encriptado. Muchas de ellas pueden descargarse en la red de manera gratuita.

Antes de introducir cualquier dato personal es recomendable ver si la url del sitio que vamos a visitar empieza por http:// y si está usando el protocolo de seguridad adecuado.



la red Wi-Fi que el usuario ve en el listado de redes disponibles de su sistema operativo, tiene el patrón WLAN_XX, donde XX son los dos últimos caracteres de la clave secreta. El resultado es que nueve de los trece dígitos se pueden deducir.

Un paso adelante: WPA

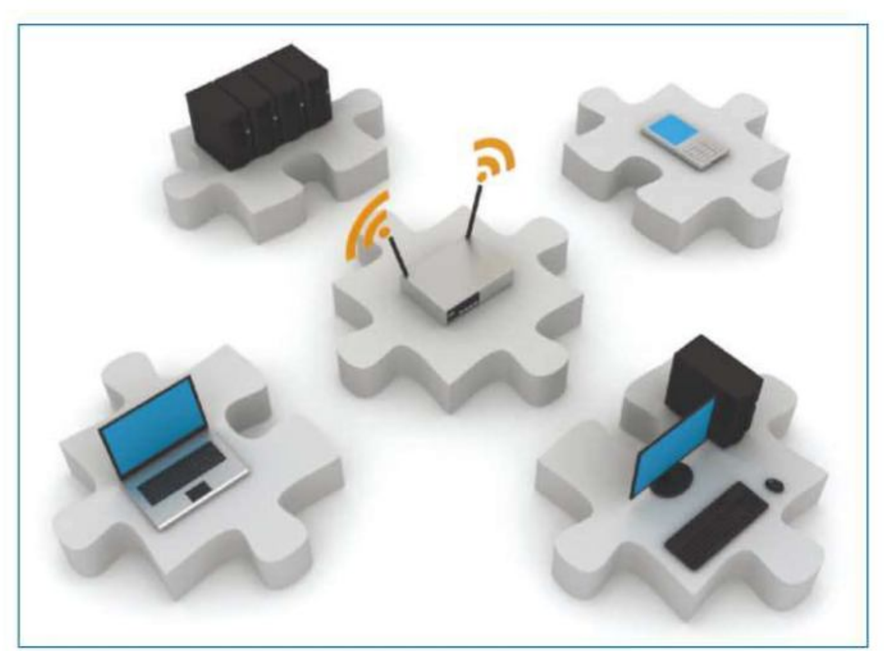
Con el fin de perfeccionar el sistema WEP, surgió este protocolo que funciona adoptando la autentificación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.

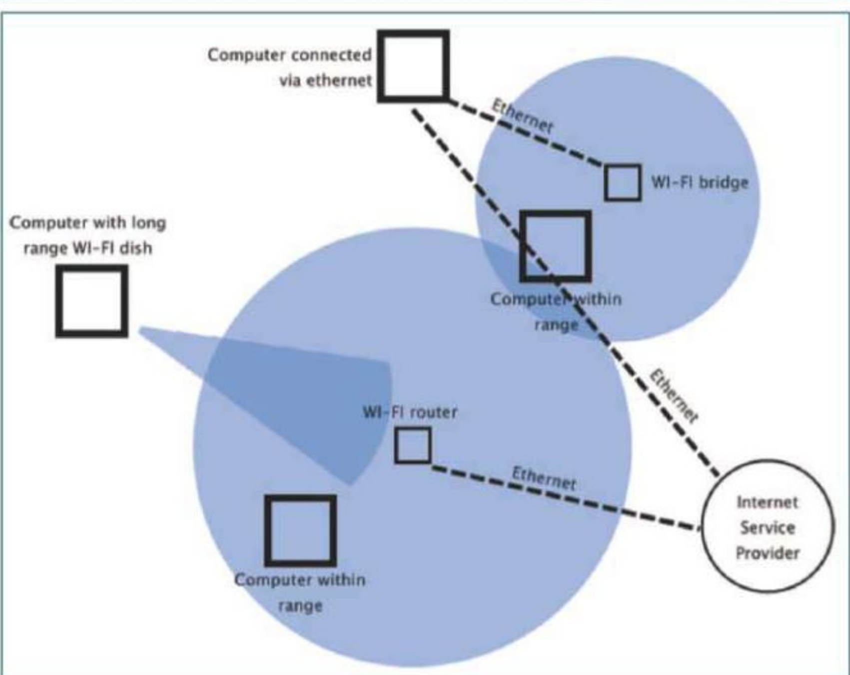
Una de las mejoras que ofrece sobre WEP es la implementación del Protocolo de Integridad de Clave Temporal (TKIP- Temporal Key Integrity Protocol), que se encarga de modificar claves dinámicamente a medida que se utiliza el sistema.

Además, cuando se combina con un vector de inicialización mucho más grande evita los ataques de recuperación de clave.

En lo que se refiere a los procesos de autentificación y cifrado, la comprobación de redundancia cíclica (CRC- Cyclic Redundancy Check) que se utiliza en WEP es poco seguro, ya que se puede alterar la información y actualizar la CRC del mensaje sin saber cual es la clave WEP. WPA implementa un código de integridad del mensaje, haciendo mucho más complicado que esto ocurra.

Pese a alas notables ventajas que implica sobre WEP, está bastante menos extendido. Según Inteco (Instituto Nacional de Tecnologías de la Comunicación) solo uno de cada cinco usuarios lo utiliza. Por contra, este mismo estudio rebela que más del 25% de las personas sigue usando el protocolo antiguo.





WI-FI Range Diagram

Guía para lograr una conexión inalámbrica segura

Son varios los pasos que deben darse si se quiere asegurar una protección al tráfico de datos y a la conexión vía Wi-Fi. A continuación, proponemos varias medidas que se pueden tomar:

· **Cambia la contraseña por defecto:** Al adquirir un router, todos los fabricantes traen establecido por defecto un password con el que acceder a la administración del Punto de Acceso. Como el fabricante va a utilizar siempre la misma contraseña para todos los equipos, es fácil que alguien pueda conocerla.

· **Utilizar la encriptación WEP/WPA:** Ya se explicó con anterioridad las diferencias entre ambos protocolos. Es necesario que, ya sea uno u otro, el cifrado de datos sea de 128 bits. Muchas veces vienen desconectados por defecto, lo que hace necesario al usuario configurarlos una vez instala el router.

· **Ocultar la red Wi-Fi:** Para ello es recomendable hacer dos cosas. La primera de ellas es cambiar el SSID, es decir, que en lugar de que ponga "linksys" o "d-link", el usuario utilice el nombre en clave que escoja. De este modo captará menos la atención de intrusos. En segundo lugar, sería bueno desactivar también el broadcasting SSID. Éste hace que un ordenador con conectividad Wi-Fi detecte automáticamente los datos de la red inalámbrica. Al modificarlo será necesario que se introduzca de manera manual en la configuración de cada nuevo equipo con el que se quiera acceder a la Red.

· **Evitar la conexión de personas no autorizadas.** En primer lugar habría que activar el filtrado de direcciones MAC (Media Access Control). Son identificadores únicos de cada ordenador, por lo que al



utilizar este sistema, se puede permitir que accedan a la Red tan sólo aquellos dispositivos que el gestor haya especificado de manera previa. Asimismo, se puede establecer un número máximo de equipos conectados al mismo tiempo.

• Finalmente, **para ser extremadamente cauteloso**, se pueden llevar a cabo una serie de acciones complementarias. Una de ellas es desconectar el punto de acceso cuanto no se utilice. Al guardarse la configuración, no será necesario introducir la clave de nuevo cuando se conecte.

Otro factor que añade más seguridad es cambiar las claves WEP cada dos o tres semanas. Es un proceso sencillo que apenas conlleva esfuerzos pero que, sin duda, asegura una máxima protección de la Red.

En resumen

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debida a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de inteferencias.

Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o muy vulnerables a los crackers), sin proteger la información que por ellas circulan.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son:

Utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP y el WPA, que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos

WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire.

WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud

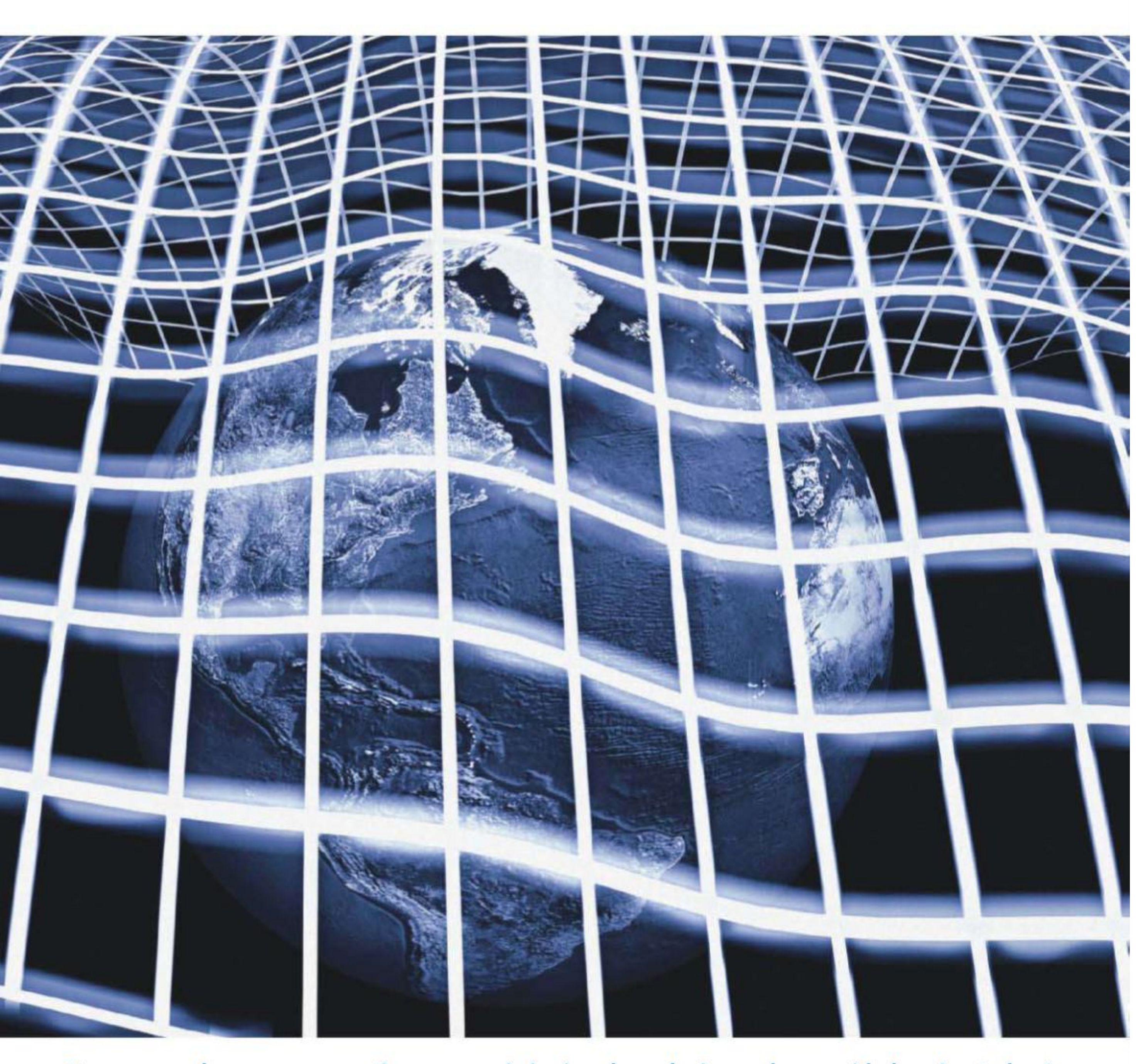
IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados.

Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios. El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

Seguridad perimetral La defensa más eficaz



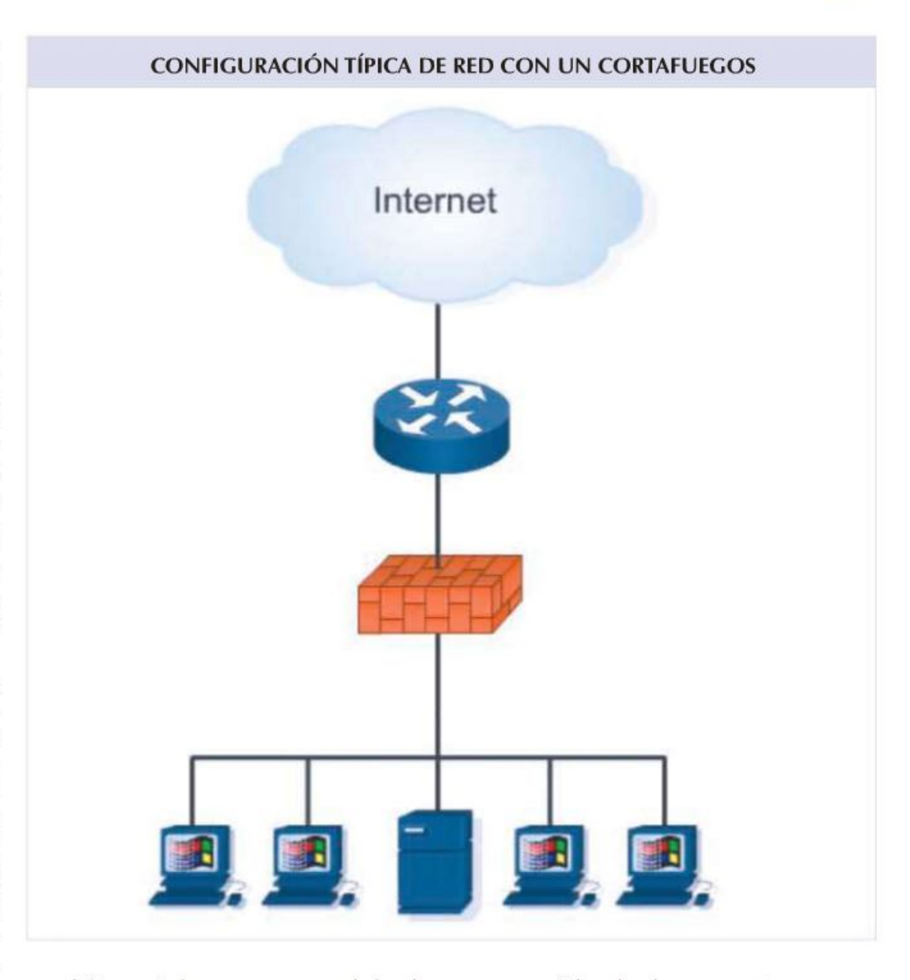
Pese a que algunas voces sostienen que ni siquiera las soluciones de seguridad perimetral más potentes ofrecen ya la protección necesaria, está claro que siguen siendo el pilar sobre el que se sustentan las defensas de muchas empresas ante la infinidad de amenazas que acechan a sus sistemas informáticos.



Las tecnologías en materia de seguridad avanzan y lo hacen a un ritmo vertiginoso, pero esta circunstancia no implica que las amenazas se queden rezagadas; más bien al contrario, lo que hacen es transformarse en un peligro cada vez más sofisticado y complejo. En este círculo vicioso, la seguridad adquiere un protagonismo fundamental dentro de las empresas, que deben poner infinidad barreras para mantener a dichas amenazas lo más lejos posible. Aquí es donde entran en acción las soluciones de seguridad perimetral, que basan su funcionamiento en la protección del sistema informático de un negocio desde fuera; es decir, se trata de establecer una especie de "caparazón" que proteja los elementos sensibles frente a amenazas de todo tipo, como virus, gusanos, troyanos, ataques de denegación de servicio, robo o destrucción de datos o el pirateo de páginas web, por citar sólo algunas de las más comunes y frecuentes.

De hecho, según la consultora IDC, los ingresos para este segmento se incrementarán hasta los 7.300 millones de dólares a finales de 2010, lo que significa una media anual de crecimiento del 11%. Esto es posible porque las grandes y pequeñas compañías se van concienciando cada vez más de la necesidad de disponer de soluciones de seguridad para proteger sus sistemas. Saben que el peligro, aunque también se encuentra dentro, proviene sobre todo del exterior. Al respecto, la consultora Lightspeed publicó a comienzos de año un estudio sobre el origen de los riesgos que corren los sistemas, según el cual los ataques internos representaron un 66% durante 2006 y tan sólo un 24% en 2007, y se espera que en 2008 se produzca un nuevo descenso. Esto no hace más que demostrar el creciente número de amenazas y ataques externos a los que se enfrentan los sistemas y las redes empresariales y que infectan equipos, roban información confidencial, crean denegaciones de servicio o causan interrupciones de red, entre otras costosas acciones. Por este motivo, la seguridad perimetral se presenta como una opción necesaria en todas las empresas, ya que evita riesgos procedentes de Internet. Además este tipo de protección ofrece beneficios como liberar de trabajo a servidores y estaciones de trabajo, optimizando recursos, así como aumentar la productividad de los usuarios, evitando tráfico innecesario dentro de la red.

CONFIGURACIÓN TÍPICA DE RED CON UN CORTAFUEGOS



Antes de que surgiera Internet, el correo electrónico y el comercio electrónico, la naturaleza cerrada de las redes corporativas hacía de la seguridad un tema relativamente fácil. El modelo de defensa clásico giraba en torno a defender una red interna confiable del exterior.

Los riesgos a los que están expuestos las redes informáticas han evolucionado al mismo ritmo que lo ha hecho la tecnología. Las variaciones sobre las distintas amenazas son incontables y crecen día a día, poniendo en peligro a cualquier ordenador.

Según un estudio realizado por eMedia USA para GFI Software a finales del año pasado, cuatro de cada diez pequeñas y medianas empresas de Estados Unidos no creen que sus redes sean seguras, a pesar de tener instaladas aplicaciones antivirus (96%), antispam (80%) y cortafuegos (93%). Esto indica, según GFI, que las pymes están comenzando a dudar de la efectividad de los productos tradicionales de seguridad perimetral como protección ante amenazas, incluyendo las fugas de información y brechas de seguridad en las redes. De hecho, el 39% de los encuestados considera a los correos infectados de virus como el mayor riesgo para la seguridad de la red, seguido de las descargas de Internet (22%) y los intentos de hacking (10%). Sólo el 7% apuntó a los ataques internos y las amenazas de los dispositivos portátiles de almacenamiento como la fuente de mayor peligro.

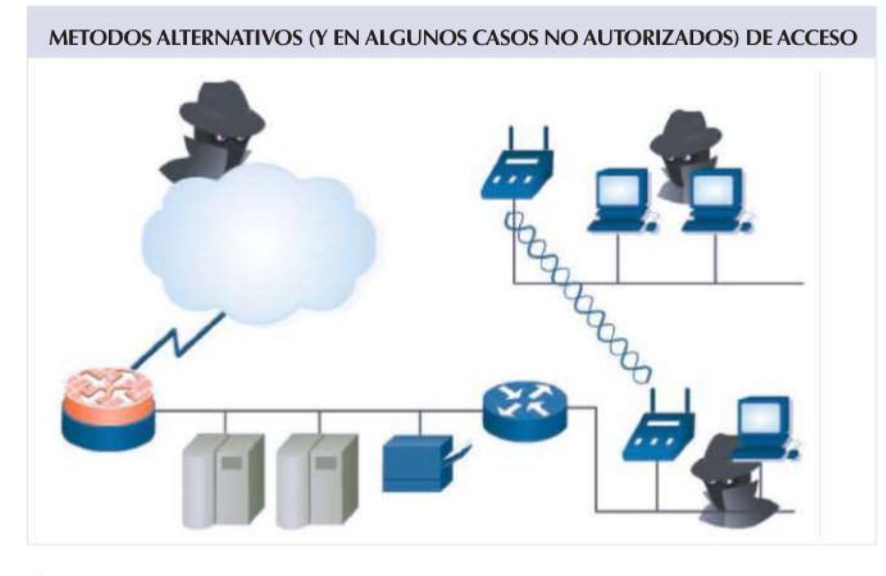
En seguridad de redes, los usuarios son el eslabón más débil, por lo que su comportamiento dentro de la empresa tendrá una repercusión en la seguridad de la compañía. Por tanto, uno de los aspectos que habría que mejorar en este sentido, según el directivo, es el conocimiento en materia de seguridad. Mientras que los administradores informáticos están mejor preparados y saben lo que se debería y lo que no se debería hacer, los empleados no lo conocen, ya que no cuentan ni con una gran experiencia tecnológica ni demasiado interés en los temas relacionados con la seguridad. No basta, pues, con que el departamento informático esté al tanto de las últimas amenazas contra la seguridad informática. Se debe formar a los empleados para que no abran correos electrónicos sospechosos o para que no faciliten información personal o corporativa como respuesta a un mensaje que lo solicita sólo porque parezca genuino, por poner algún ejemplo.

Si toda la plantilla siguiera unas buenas prácticas básicas en seguridad, el número de problemas relacionados con la se-

CONEXIÓN DE SUCURSALES, PROVEEDORES Y USUARIOS REMOTOS.

CONEXIÓN DE EXTRANETS

METODOS ALTERNATIVOS (Y EN ALGUNOS CASOS NO AUTORIZADOS) DE ACCESO



EN LA INFERIOR SE HA CONFIGURADO YA UN PUNTO DE GESTIÓN CENTRALIZADO QUE PUEDE DOTAR A LA RED DE MECANISMOS DE SEGURIDAD PERIMETRAL

guridad en las empresas descendería de manera notable. No en vano, la mencionada encuesta revela que el 32% de las empresas encuestadas habían sufrido una brecha en los últimos doce meses, principalmente debido a ataques de virus (69%), seguido por descargas de Internet infectadas (30%) y pérdidas de hardware, como portátiles (24%).

Así las cosas, no resulta extraño que la mayoría de las pequeñas y medianas empresas consultadas (90%) se conformen con instalar una solución software; mientras que sólo un 55% aseguraron optar por una combinación de software, dispositivos y servicios hospedados Ante esta situación, no resulta extraño que la mayoría de las empresas coincidan en afirmar la importancia que tiene para las organizaciones la necesidad de desplegar un plan preventivo de seguridad informática entendido como un todo. La estrategia más efectiva es aquélla que protege de manera integral toda la red. Para ello, es necesario salvaguardar los puntos finales, pero también es indispensable una política de seguridad estructurada sobre los pilares de formación de personal, creación de protocolos y automatización, todo ello sustentado sobre una buena base técnica de software y también hardware. De poco sirve, por ejemplo, una red totalmente blindada hacia amenazas externas si no disponemos de un buen plan de prevención de pérdida de datos que garantice la disponibilidad y, por tanto, la continuidad.

Así las cosas, todas las funcionalidades de seguridad perimetral y análisis de contenidos son necesarias, con integración entre sí para permitir la cobertura de cualquier ataque mixto y con el rendimiento suficiente para no introducir retardos en las redes que hay que proteger. Estos productos generan una serie de ventajas para las compañías, entre las que se encuentran una protección completa de las redes, tanto en la conexión como en la aplicación; un menor coste total de propiedad, no sólo en infraestructura, sino en servicios de soporte, mantenimiento y formación del personal; y una gestión desde una plataforma única y centralizada.



Ahora bien, lo que hay que explicar a las compañías es que cualquier modelo de seguridad debe de venir precedido de «un análisis exhaustivo de las necesidades de cada empresa y de sus puntos críticos y, también, de que la mejor protección es aquélla que salvaguarda todos y cada uno de esos puntos críticos.

Y es que si una organización es capaz de fijar el punto donde tiene sus principales activos, es posible identificar cuáles son las amenazas y vulnerabilidades más urgentes. De este modo, pueden concentrar su atención e inversiones donde más lo necesitan. Esto facilita la construcción de conocimientos especializados, la seguridad de la red y la creación de planes estratégicos para mantener los nuevos programas de seguridad o los ya existentes.

Seguridad adaptativa y UTM

Una vez establecidos los puntos donde se quiere hacer foco y definido el plan de seguridad perimetral adecuado a cada empresa, hay que considerar cómo realizar el despliegue. El objetivo es conseguir una seguridad adaptativa basada en tres conceptos: defensa multinivel, gestión unificada ante amenazas y garantía de continuidad de negocio. La clave reside en integrar la posibilidad de clusterización desde la base, con el objeto de garantizar la escalabilidad, la continuidad de servicio y el mantenimiento sin paradas». Todo ello, por supuesto, sin olvidar que la fortaleza de un sistema de seguridad perimetral radica «tanto en la potencia de sus motores de cortafuegos, análisis de contenidos y control de acceso como en la facilidad de la gestión, con el fin de evitar errores y disponer de información inteligible que ayude a saber qué pasa en la red de forma sencilla y, por tanto, aclare qué decisiones conviene tomar.

Siguiendo esta máxima de facilidad de gestión, están copando el mercado una serie de soluciones multifunción, denominadas UTM (Unified Thread Management), que pretenden ir más allá del antivirus y el firewall y añadir otros métodos de seguridad, todo ello concentrado en un único dispositivo. Este tipo de soluciones son cada vez más completas, e incluyen funciones de antispyware, creación de túneles VPN SSL e IPSec, sistemas de detección y prevención de intrusiones, antiphishing, gestión de logs, consola de gestión centralizada, etc.

De este modo, permiten tener concentrada la seguridad informática de la red en un solo dispositivo, lo que implica un ahorro en el tiempo de instalación, mayor interoperabilidad entre los elementos que conforman el sistema de seguridad, facilidad para la detección de problemas, actualizaciones rápidas y sencillas. Todo ello, además, configurando su disponibilidad para evitar el riesgo que supone tener un único punto en el que se concentra todo el sistema de seguridad.

Básicamente, existen dos grandes grupos de peligros procedentes del exterior: a nivel de red y a nivel de contenidos. Esta clara división ha propiciado que los fabricantes de seguridad perimetral se centrasen en la creación de dispositivos para uno u otro fin.

Las primeras son transmisiones que, con sólo establecerse, entrañan un riesgo para la red de la compañía, pues implican el uso de recursos o datos internos por parte de personas ajenas a la misma.

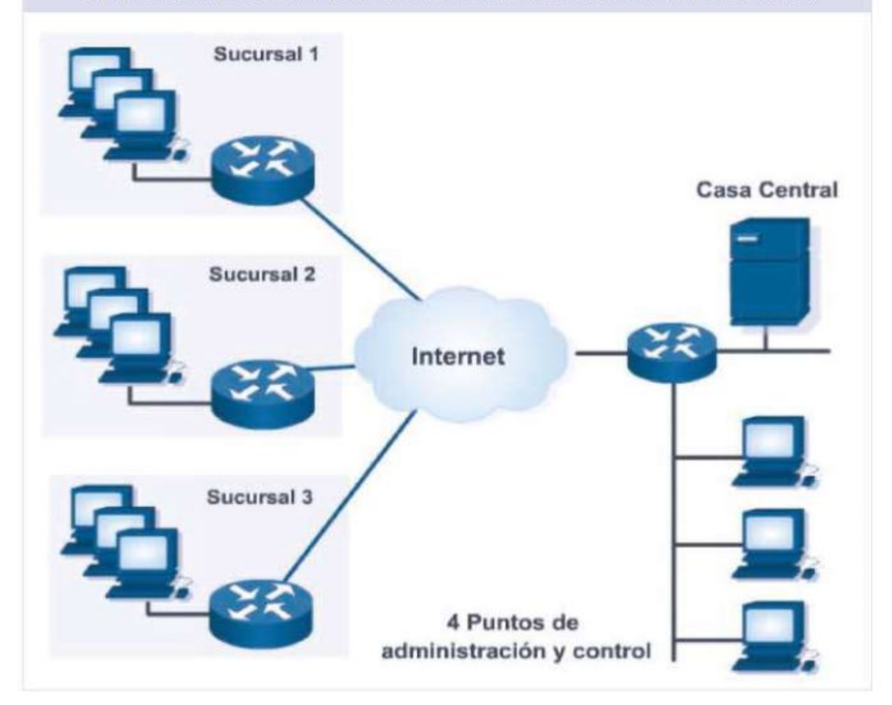
>>> UTM, LA GRAN ESTRELLA

Como hemos apuntado, los sistemas UTM son actualmente una excelente salida para una pyme cuyas exigencias en materia de seguridad informática no sean especialmente elevadas. Al no disponer ni de personal dedicado ni de una partida presupuestaria asignada a tal efecto, los pequeños y medianos negocios tienden a la implantación de estas soluciones, que garantizan una gestión unificada de las amenazas al incorporar en un solo dispositivo protección anti-malware, anti-spam, anti-phising, filtrado de contenido web, además de cortafuegos y VPN preconfigurados.

Con una solución de este tipo, una pyme consigue simplificar las labores de administración y gestión en el entorno de seguridad, además de solventar elegantemente el despliegue de complejas soluciones y reducir el coste total de propiedad. Aún así, parece aventurado afirmar que los sistemas UTM sean la panacea. A todas luces, resultan insuficientes para una gran empresa, y en determinados entornos, cuando se ven sometidas a situaciones de alta carga de trabajo, sufren una merma en su rendimiento debido a la gran cantidad de operaciones que han de realizar.

La realidad es que no hay soluciones definitivas, ya que los hackers están buscando, en todo momento, las vulnerabilidades a explotar, y los productos deben ir adaptándose a la naturaleza de los ataques que surgen. En este sentido, UTM está teniendo muy buena acogida, pero hablar de que sean la solución definitiva quizá sea demasiado, pues en seguridad no existen garantías totales, más que nada por el espectro de amenazas que acechan la red y por el ritmo al que avanzan.

CENTRALIZACIÓN DE LOS PUNTOS DE ADMINISTRACIÓN Y CONTROL



>>> AMENAZAS MÁS FRECUENTES

AMENAZAS A NIVEL DE RED

Conexiones no permitidas: Todas las conexiones entre equipos de la red y el exterior deben ser permitidas y conocidas por el administrador de la misma.

Robo de información en las transmisiones: La comunicación entre dos ordenadores conectados a Internet se lleva a cabo a través de TCP/IP, un protocolo muy eficaz y extendido, pero muy inseguro, por lo que existen infinidad de sistemas para poder espiar la comunicación entre máquinas. La solución son las técnicas de cifrado y encriptación.

Intrusiones y ataques de hackers: Las aplicaciones que más los sufren son tan habituales y conocidas como clientes de correo, programas de mensajería instantánea o el software P2P.

AMENAZAS A NIVEL DE CONTENIDOS

Malware: Se trata de programas que son capaces de causar algún tipo de daño en los equipos donde se ejecutan. Los códigos maliciosos pueden adoptar infinidad de formas, como virus, gusano, troyano, spyware, dialers, phising, jokes o amenazas combinadas.

Contenidos potencialmente peligrosos: Se trata de ficheros o correos recibidos en la red cuya confiabilidad es incierta. Llegan a la red a través de navegación web o e-mail.

Spam: Es el correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. El daño puede cuantificarse económicamente en horas de trabajo que se malgastan cada día en la tarea de leer y eliminar dichos mensajes basura.

Contenidos web no deseados: Además de ser una herramienta de trabajo, Internet también supone un motivo de distracción para los trabajadores, por lo que controlar los contenidos web a los que se accede es vital para evitar pérdidas de productividad.

La combinación de un firewall o cortafuegos con una VPN (red privada virtual) es, desde siempre, la solución más recurrida, a la que se han ido añadiendo complementos posteriormente, como los sistemas IDS (Intrusion Detection Systems) e IPS (Intrusion Prevention Systems).

Por su parte, las amenazas a nivel de contenidos siempre van asociadas a datos que alcanzan la red por vías aparentemente inocuas, como la navegación web o el correo electrónico.

Las formas en que pueden afectar a las compañías son muy variadas y van desde el código malicioso a los contenidos potencialmente peligrosos, pasando por el correo basura.

En este caso, las soluciones pasan por los conocidos antivirus, antispam y las soluciones de filtrado, o los más recientes appliances basados en SCM (Secure Content Management), que garantizan una protección especializada, de forma desatendida y sin influir en el funcionamiento de la red corporativa.

Respuesta de la tecnología

Sin embargo, las amenazas actuales más sofisticadas utilizan combinaciones de ambos tipos de ataques para explotar los puntos débiles de sistemas operativos y aplicaciones de amplia difusión, comprometiendo así a las redes en las que residen y sus recursos, con resultados en ocasiones devastadores.

Igualmente, también son capaces de detectar las vulnerabilidades de los servidores y se transmiten y extienden a través de las redes a una velocidad increíble, al utilizar más de un vector de ataque y esconderse dentro del contenido de archivos y navegación descargados por los propios usuarios.

No es, por tanto, posible luchar contra dichos ataques mediante soluciones de seguridad convencionales, como un cortafuegos o un antivirus, sino que es necesario utilizar dispositivos multipropósito, como routers multiservicio o sistemas UTM (Unified Threat Management).

Así, se ha percibido una clara evolución en el mercado desde lo que llamamos seguridad perimetral a una defensa en profundidad, con el auge de soluciones conjuntas que combinan las técnicas de detección, prevención y mitigación de ataques, ya que soportan funcionalidades de firewall, VPN, IPS y Anti-X (anti-virus, anti-spam, anti-phising, anti-spyware, filtrado de contenidos y sitios web).

Las soluciones de seguridad son cada día más diversas y complejas, a la vez que se caracterizan por un uso transparente e invisible, de manera que no interfieran con el ritmo habitual de trabajo.

¿Qué demandan las empresas?

Las compañías españolas se están concienciando progresivamente de que resulta imprescindible una correcta inversión en seguridad, pues las amenazas afectan a todas las compañías por igual, sin distinguir tipos, sectores ni tamaños.

Asimismo, el control y el seguimiento de los datos se han convertido en una práctica de negocio obligatoria merced al nuevo entorno regulatorio.

Y el principal dinamizador del mercado es la aparición de aplicaciones de intranet para facilitar el acceso remoto aprovechando la banda ancha del ADSL, el cable o Wi-Fi. Ante este panorama, la pregunta que surge es clara: ¿qué servicios y soluciones de seguridad perimetral tienen una mejor salida? Para responderla, obviamente, hay que distinguir entre grandes compañías y pymes: en las corporaciones de mayor tamaño, las appliances dedicadas han cobrado bastante importancia por su alto rendimiento y el grado de protección para aplicaciones de misión crítica; en la pequeña y mediana empresa, UTM se está implementando de forma masiva, al paquetizar en un solo producto herramientas para hacer frente a diferentes riesgos.

Las grandes cuentas quieren soluciones dedicadas que separen la defensa de red de la de contenidos, escalables y especializadas según el tipo de tráfico o de protección; mientras, las pymes optan por aplicaciones que centralizan el mayor número de herramientas en un único dispositivo, fáciles de usar y gestionar.

Una defensa completa

Como ya hemos comentado, un sistema básico de seguridad perimetral debe contemplar protección ante intrusiones externas e internas, una custodia eficaz y lógica de la información privada y medidas contra el malware. Una solución robusta incorpora elementos tan cotidianos como firewalls, VPNs o zonas desmilitarizadas (DMZs), a los que se han ido incorporando los IDS e IPS para la supervisión del acceso exterior, o los SCM para la gestión de contenidos.

Además, cada vez se apuesta más por la colaboración y la movilidad, lo que supone un reto para la seguridad, ya que se abren muchos nuevos frentes a los que atender. Todo esto se traduce en gran crecimiento en las ventas de routers con seguridad integrada, soluciones UTM para sustituir a los cortafuegos y equipos con soporte de VPN SSL. Además, el mercado está asimilando las ventajas que aporta la activación de una política de control de admisión

LAS GRANDES CUENTAS QUIEREN SOLUCIONES DEDICADAS QUE SEPAREN LA DEFENSA DE RED DE LA DE CONTENIDOS, ESCALABLES Y ESPECIALIZADAS SEGÚN EL TIPO DE TRÁFICO O DE PROTECCIÓN; MIENTRAS, LAS PYMES OPTAN POR APLICACIONES QUE CENTRALIZAN EL MAYOR NÚMERO DE HERRAMIENTAS EN UN ÚNICO DISPOSITIVO, FÁCILES DE USAR Y GESTIONAR. ADEMÁS, CADA VEZ SE APUESTA MÁS POR LA COLABORACIÓN Y LA MOVILIDAD, LO QUE SUPONE UN RETO PARA LA SEGURIDAD, YA QUE SE ABREN MUCHOS NUEVOS FRENTES A LOS QUE ATENDER.

en la red (NAC).A pesar de todo, muchas empresas todavía tienen que cambiar su mentalidad y comprender que el presupuesto destinado a soluciones de seguridad es una inversión, y no un gasto.

En los últimos años, la conciencia sobre la necesidad de implantar medidas de seguridad ha aumentado, pero aún queda mucho por hacer en todos los sentidos, un largo recorrido hasta que se considere la seguridad como una inversión, no como un gasto.

¿Es la seguridad perimetral suficiente?

Por desgracia, hoy por hoy las defensas perimetrales ya no parecen ser suficientemente eficientes. Un único usuario móvil y su portátil pueden causar innumerables problemas a una empresa.

Por ejemplo, si usa su ordenador en el sitio de un cliente y contrae una infección. Al regresar a la oficina, se conecta a la red interna, con lo que la seguridad perimetral ya ha sido físicamente traspasada y la infección es libre de expandirse a otros equipos. Por esta razón, resulta esencial que las redes corporativas integren mecanismos internos que protejan el negocio frente a este tipo de situaciones. Lo cierto y verdad es que actualmente una red no puede protegerse simplemente asegurando su perímetro.

A medida que las empresas han ido consolidando sus centros de datos, creando redes convergentes y adoptando Internet, su entorno ha quedado abierto a los socios y partners a través de las extranets, las conexiones con los puntos de venta y los empleados que trabajan en casa, por citar algunos ejemplos.

En seguridad, nunca es posible hablar de una protección del 100%; más que hablar de la eficiencia de la seguridad perimetral, quizás sería necesario analizar si la inversión realizada en la misma es realmente suficiente. Resumiendo, y por todo lo dicho, se presenta como una cuestión vital tener un control absoluto de las comunicaciones que se establecen a través del perímetro, sabiendo quién accede y a qué información puede hacerlo.

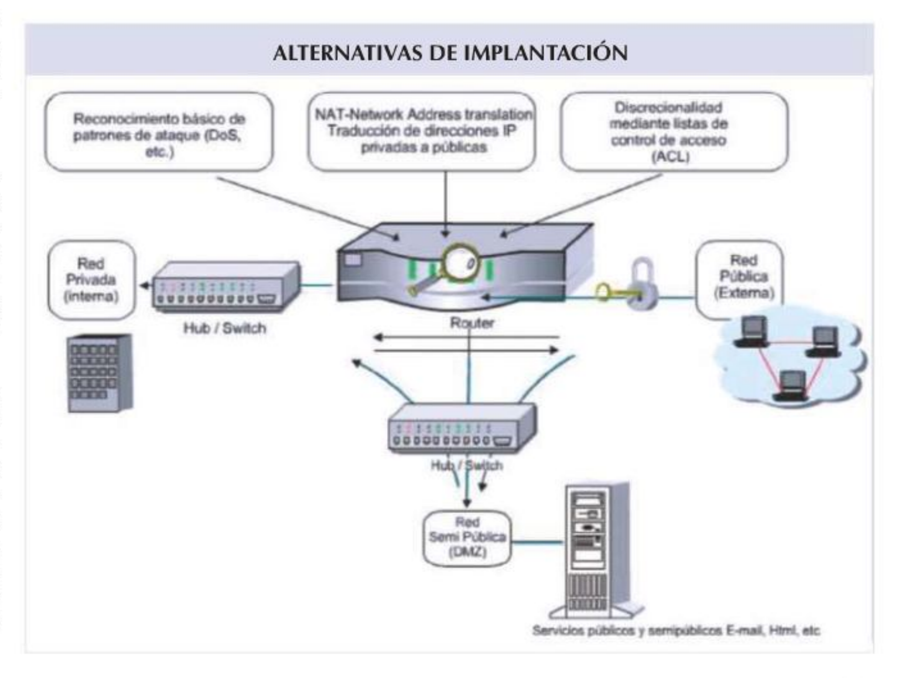
No hay que olvidar que la seguridad perimetral, aunque muy importante y necesaria, no deja de ser una más de las capas de protección de una red corporativa, que sólo es eficaz si se complementa con otras capas.

Mirar el futuro

Sin embargo, el futuro de este mercado no pasa sólo por la seguridad gestionada. La seguridad seguirá el camino de la protección basándose en entornos virtuales. Se trata de satisfacer la necesidad del cliente: máxima protección sin mermar el rendimiento y ahorrando costes y espacio en el CPD. Con el desarrollo de estos sistemas, los equipos que conforman la red corporativa de cualquier empresa serán capaces de incrementar las funcionalidades de detección automática de anomalías, y de solucionar autónomamente los problemas detectados en el uso de la misma», explica.

A pesar de todo, resulta muy difícil saber cómo evolucionarán las amenazas, pues a cada paso de la industria de la seguridad le sigue otro de la del malware, con lo que más que centrarse en el futuro lejano, lo realmente conveniente es atender a mejoras continuas y constantes. En este sentido, es posible establecer varias pautas que toda solución de seguridad perimetral debe ser capaz de cumplir, y en torno a ellas seguirá girando el mercado: Facilitar la gestión centralizada sin importar la ubicación de la red ni la solución de seguridad que hay que gestionar; proteger con idéntico grado de seguridad a las oficinas distribuidas y a las sedes centrales; y ofrecer soporte para entornos virtualizados. Además, este tipo de soluciones incluirá cada vez más características, integrándose como una capa más del servicio, siendo capaces de manejar más tipos de tráfico y con mayor granularidad y control de los usuarios, teniendo en cuenta tanto el tráfico entrante como el saliente e incluyendo capas de reporting que permitan seguir las regulaciones que cada vez con más frecuencia deben cumplir las empresas. Por último, todo ello se combinará con la externalización de la gestión de toda la seguridad de una empresa, excepto aquellas funciones que sean realmente diferenciales y estratégicas para el negocio.

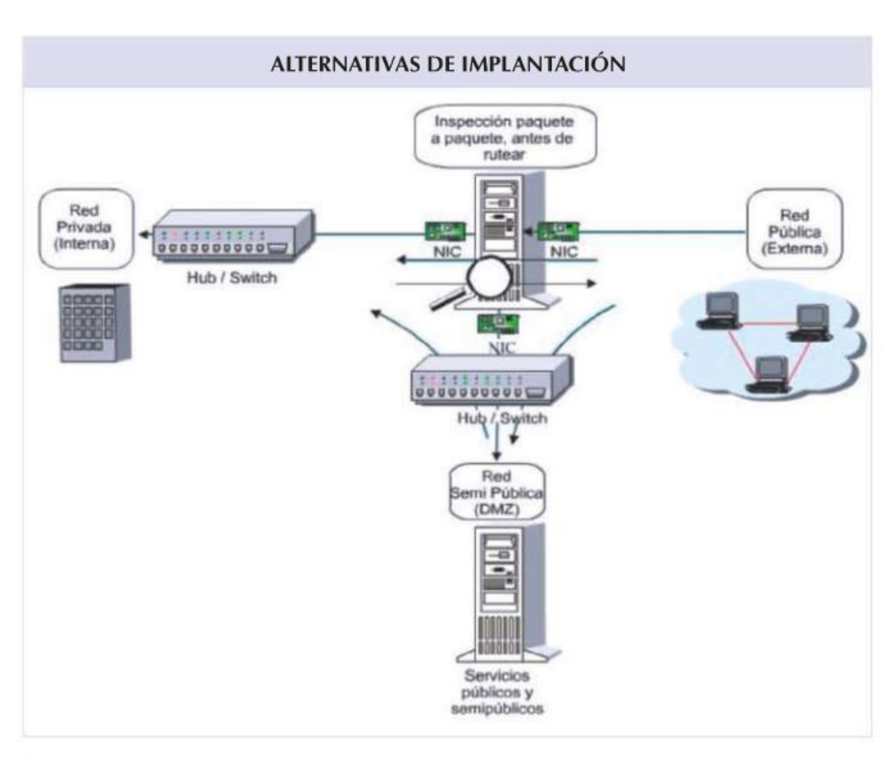
El verdadero problema va a llegar a partir de ahora, en plena crisis financiera y eco-



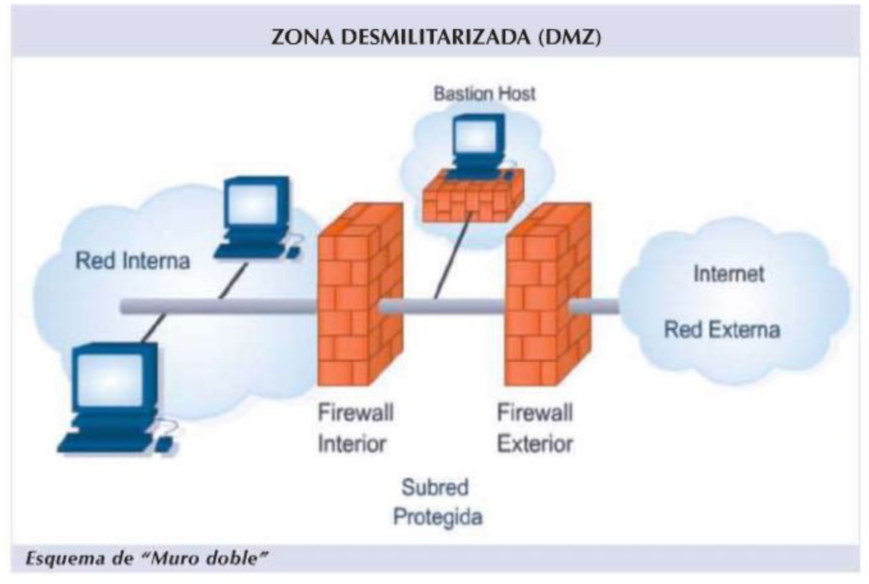
nómica mundial, que hará reducir los presupuestos destinados a seguridad tanto de grandes como de pequeñas y medianas empresas. No en vano, el temor generalizado en la industria es que así sea. Nadie sabe lo que va a suceder, pero lo que sí es evidente es que el cuarto trimestre del año será el auténtico termómetro, dado que si los crecimientos son bajo, debemos prepararnos para lo peor. Sin embargo, sí existe un sentimiento generalizado de que el mercado de la seguridad es tan importante para cualquier empresa que sería una de las partidas presupuestarias que no se toquen.

Así pues, si hasta no hace mucho la tónica general era la de favorecer la inversión en soluciones de seguridad que protejan sus infraestructuras e información, ahora la situación por la que atraviesa la economía no está siendo muy favorable a las inversiones en general. Aunque ante la constante aparición de nuevos ataques y las pérdidas que están provocando, es posible que las compañías, cuando menos, mantengan su presupuesto en seguridad o lo incrementen, dando prioridad a esta área frente a otras. Sin embargo, el énfasis de las empresas se focaliza mucho más en la optimización de sus operaciones tratando de mantener su presencia en el mercado. Desde esta perspectiva, vemos que las organizaciones focalizarán sus presupuestos en hacer más eficientes sus infraestructuras, en mejorar la colaboración entre sus empleados y en potenciar las capacidades existentes. Contar con una plataforma de seguridad eficiente en este caso representa una solución que permite a las compañías obtener los beneficios antes expuestos. Claro que hay quien, en estos momentos de incertidumbre económica, lanza una recomendación a las empresas: Es ahora cuando «las compañías necesitan ser más selectivas y rastrear el mercado en busca de un proveedor que suministre productos eficaces a precios competitivos. El mayor error es dejar que los presupuestos se metan en el camino de la seguridad, ya que el coste que supone una brecha siempre será muy superior al de una solución informática. Como respuesta a esta tendencia cada vez más extendida de la externalización de la seguridad está surgiendo un nuevo concepto que se denomina seguridad gestionada, cuyo objetivo es, según Román, de Fortinet, «ofrecer a las empresas disponibilidad, integridad y confidencialidad en todas sus comunicaciones mediante la gestión y monitorización integral de sus sistemas de seguridad». Asimismo, este modelo permite que las compañías no se vean obligadas a realizar grandes inversiones para adquirir equipamiento de seguridad, renovaciones costosas o mejoras en la formación específica de sus empleados, entre otros. Así pues, las compañías que gestionan este tipo de seguridad ponen al alcance de las organizaciones posibilidades adaptadas a cada necesidad particular, entre las que destacan cortafuegos gestionados, VPN gestionadas, detección de intrusión gestionados, tráfico de correo limpio, antivirus gestionados, filtrado de contenidos y páginas web, auditoría de seguridad continua o de backup y alojamiento de datos. Con el tiempo, este sistema irá ampliando su oferta de servicios, pero por ahora no deja de ser un método eficaz para asegurar y tener un control de la red corporativa.

ALTERNATIVAS DE IMPLANTACIÓN



ZONA DESMILITARIZADA (DMZ)



Esquema de "Muro doble"

EN SEGURIDAD, NUNCA ES POSIBLE HABLAR DE UNA PROTECCIÓN DEL 100%; MÁS QUE HABLAR DE LA EFICIENCIA DE LA SEGURIDAD PERIMETRAL, QUIZÁS SERÍA NECESARIO ANALIZAR SI LA INVERSIÓN REALIZADA EN LA MISMA ES REALMENTE SUFICIENTE Y EVALUAR QUÉ RIESGOS NO SE PUEDEN ASUMIR NUNCA Y CUÁLES SÍ.



La crisis llega a la industria del malware



La crisis está afectando a la práctica totalidad de sectores económicos, y la industria del malware no es una excepción. Según los datos recabados por los laboratorios de seguridad de G Data, el precio en el mercado negro de los servicios de envío de spam ha caído hasta prácticamente la mitad en el primer trimestre de 2009, respecto al mismo periodo del año anterior.

Si en los tres primeros meses de 2007 se pedían 350 euros por enviar 20 millones de correos no deseados y en 2008 su precio ya bajó a 290 euros, ahora tan sólo son necesarios 150 euros para contratar este tipo de servicios fraudulentos.

Este descenso de precios en los servicios ofertados por la industria del malware hace preveer una nueva avalancha de ataques, al ser más asequibles. Por ello, y en línea con la coyuntura económica actual, los fabricantes también tenemos que mover ficha, y en consecuencia desde G Data hemos bajado el precio de nuestras soluciones. Todos los esfuerzos que se encaminen a frenar esta amenaza serán bienvenidos.

La crisis, principal señuelo del spam

Al mismo tiempo, los creadores de malware, aprovechándose como siempre hacen de los asuntos de mayor actualidad, están recurriendo a nuevos ganchos para distribuir código malicioso. Por ello, aquellos que buscan trabajo o necesitan dinero son la presa perfecta, y el spam está recurriendo a asuntos como falsas ofertas de trabajo o créditos bancarios trampa para aumentar su difusión.

Según los datos de los que disponemos, en este momento uno de cada cuatro correos electrónicos no deseados consiste en una oferta de préstamo bancario.

A finales de 2008, apenas representaban un 3% de todo el spam enviado, mientras que ahora el 28% de estos correos recurren a este asunto como señuelo. De esta forma, el spam farmacéutico deja de ser el más habitual, tras varios años de hegemonía.

Por desgracia, no se vislumbra una solución a corto plazo para esta lacra, y de hecho en lo que llevamos de año el 72% de todos los correos electrónicos mundiales fue no deseado. En vista de estos porcentajes, se corre el riesgo de llegar a copar el tráfico de la Red, con el perjuicio que ello supondría en la utilización de una herramienta tan valiosa como Internet.

Debido a la gravedad de la situación, cada vez más países occidentales refuerzan su legislación en materia anti-spam. Tal medida está provocando que los ciberdelincuentes se estén desplazando a aquellos países más permisivos al respecto, para escapar de las consecuencias legales de enviar correos no deseados a gran escala. Ante esta situación, conviene estar atento a los servidores alojados en estos "paraísos del spam", localizados principalmente en la Europa del Este.

A cada paso que la industria del malware trate de dar, debemos ser capaces de responder con un movimiento inmediato. Sólo así lograremos minimizar la incidencia del cibercrimen.

Jorge de Miguel es responsable de G Data para España y Portugal

Cada vez más países occidentales refuerzan su legislación en materia anti-spam.

En los últimos años está aconteciendo un silencioso cambio de enormes proporciones en Internet. Los tradicionales sitios web de empresa, producto o servicio, cuyo sólo propósito es el de proporcionar contenido estático con el objetivo de transmitir información de Marketing a los clientes potenciales están dejando paso a una nueva raza de aplicaciones web altamente funcionales, capaces de proporcionar contenido dinámico, servicios a la comunidad, herramientas de colaboración e interacción, seguridad y, por supuesto, en tiempo real y con cada vez, mejor escalabilidad y prestaciones.

DotNetNuke
Una introducción al framework de aplicaciones web

(Iª Parte)

Una de estas herramientas que está surgiendo de este movimiento, motivado por los consumidores, cada vez más exigentes, las empresas y empresarios, cada vez más conocedores de Internet y sus posibilidades, es DotNetNuke que es un "Web Application Framework", una robusta librería de software que sirve de base para construir avanzadas aplicaciones web. Ah, y es "Open-Source", es decir, código abierto y, por tanto gratuito (pero sujeto a una licencia BSD, como la de Linux, siendo por tanto "casi" de dominio público - ver http://en.wikipedia.org/wiki/BSD_license para más información)

Con DotNetNuke podemos crear páginas web comerciales, de comunidades, intranets corporativas, extranets, portales CMS y aplicaciones a medida.

Como hemos comentado, la licencia de DotNetNuke es de tipo BSD, esto quiere decir que podemos copiarla, fusionarla, publicarla y distribuirla o sublicenciarla (decorarla con nuestro logotipo y venderla como nuestra, algo que mucha gente, aunque no sea ético, esta haciendo) e incluso venderla, eso sí, debe de incluir el copyright de la licencia de dotnetnuke (más información en http://www.dotnetnuke.com/Default.aspx?tabid=776).

En cualquier caso, DotNetNuke esta disponible para su descarga en el portal CodePlex, donde se ubican proyectos Open Source de todo tipo, http://dotnetnuke.codeplex.com/, además de otros tantos proyectos relacionados con DotNetNuke, también conocido por sus siglas, DNN.

DotNetNuke está construido sobre la tecnología .Net, concretamente ASP.Net 2.0 con el lenguaje de programación Visual Basic, habiendo migrado a principios del 2006 de la versión 1.1 a la 2.0 de .Net, estando actualmente utilizando actualmente .NET 3.5, aunque se ejecuta bien en hosting de ASP.NET 2.0 por su arquitectura.

La arquitectura de DotNetNuke se basa en la ENTLIB (Enterprise Library, proyecto open source orientado a la generación de "Bloques de aplicación" (Application Blocks) para implementar soluciones probadas en .Net, aplicando patrones de diseño a problemas de arquitectura de software y a problemas concretos de determinadas implementaciones.

DotNetNuke opera con todo tipo de base de datos - al utilizar el Data Access Application Block, permite trabajar tanto con SQL Server como MySQL, Oracle, y está abierto a todo tipo de base de datos.

La última versión de DNN, 5.1.1, opera en cualquier servidor que soporte ASP.Net 2.0, como por ejemplo, IIS (Internet Information Server).

Es realmente muy fácil extender DotNetNuke, y puede hacerse en cualquier lenguaje soportado por .Net, Visual Basic, C#, etc... y cabe citar que la extensión puede realizarse tanto a nivel de arquitectura como a nivel de módulos, siendo muy abierto.



En cuanto al Soporte, con solo citar que el proyecto consta de una comunidad de 707.934 usuarios (y creciendo) y una gran base de programadores profesionales dedicados a esta tecnología, está todo dicho...

El soporte para DotNetNuke siempre va a estar a mano, si tenéis alguna duda, tenéis a un enlace los foros oficiales de DotNetNuke en http://www.dotnetnuke.com/tabid/795/Default.aspx. En otro orden de cosas, el proyecto está muy bien gestionado y cada 10-15 días van saliendo versiones nuevas, bien de estabilización o bien con prestaciones y mejoras, siendo además muy fácil la actualización y migración de una versión previa a una nueva. La última versión, a fecha de escritura del artículo, ojo, es la 5.1.1 teniendo como fecha de lanzamiento el 28 de Julio del 2009, correspondiéndose al último framework de .NET, el 3.5.

Por otro lado, indicar que el primer dígito de la versión se asocia con el framework:

3 → Es una release para el .Net Framework 1.1

4 → Es una release para el .Net Framework 2.0

5 → Es una release para el .Net Framework 3.5

Esto es muy de agradecer para un proyecto de "open-source"..

Cabe destacar que se han iniciado subproyectos para cada uno de los módulos añadidos al proyecto principal, además de que podemos hallar muchos más módulos a nuestra disposición, algunos gratuitos y otros no. Seguido citamos algunos módulos que forman parte del proyecto principal, que también son gratuitos, al estar cobijados bajo la misma licencia. Estos son:

WebControls → Componentes de interfaz que permiten AJAX.

Announcements → Módulo para publicar noticias, eventos o cualquier tipo de contenido.

Blog → Módulo para implementar un Blog de forma fácil.

Chat → Módulo de Chat.

Contacts → permite gestionar una lista de contactos y mostrar información relevante.

Documents → Módulo que permite gestionar una colección de documentos e información relacionada a los mismos, permitiendo su descarga.

Events → Módulo que permite la planificación de eventos y visualización de la información relacionada a los mismos.

FAQ → Módulo de preguntas más frecuentes.

Feedback → Módulo de "contacto" básico.

Forum → Modulo de foros completamente integrado con DotNetNuke y muy potente.

Gallery → Galería de imágenes.

Media → Módulo para la reproducción de diferentes tipos de Media, video, audio, etc...

News → Módulo para la visualización de canales RSS, trabajando con cualquier tipo de formato; RSS, Atom, XML, etc...

Reports → Módulo para la realización y visualización de sencillos informes.

Repository → Potente módulo para almacenar una colección de archivos, imágenes, enlaces, texto, etc... y visualizarlo junto con información anexa al objeto en cuestión.

Survey → Módulo para hacer encuestas

Text/HTML → Módulo para mostrar cualquier tipo de contenido.

CON DOTNETNUKE ESTAMOS EN DISPOSICIÓN DE PODER CREAR PÁGINAS WEB COMERCIALES, DE COMUNIDADES, INTRANETS CORPORATIVAS, EXTRANETS, PORTALES CMS Y APLICACIONES A MEDIDA. LA LIMITACIÓN ESTÁ EN LA IMAGINACIÓN DE CADA UNO.



User Defined Table → Este módulo nos permite generar una tabla con datos, mantenerla y visualizarla como queramos.

Wiki → Este módulo nos permite generar un wiki y mantenerlo.

Por otro lado, es importante de recalcar la aceptación de DotNetNuke también; es un proyecto ampliamente utilizado en una variedad de casos y escenarios, sirviendo en ciertos casos hasta 3 (o más) millones de páginas vistas al día... DotNetNuke también permite operar con granjas de servidores, lo cual hace que sea extremadamente escalable.

Características clave

DotNetNuke nos permite, una vez descargado e instalado, gestionar inmediatamente todos los aspectos del sitio web que estemos montando, esto es así ya que nos proporciona de base todas las características clave y herramientas requeridas para operar y mantener el sitio, ofreciéndonos un completo control del mismo vía sus herramientas de administración, tanto a nivel de contenido como de estructura, estética, seguridad y gestión de miembros.. por no citarlos todos, en resumidas cuentas, estos son algunos de sus puntos clave:

Fácil de instalar y de hospedar. Está construida sobre la última tecnología de ASP.Net, pudiendo ejecutarse sobre diferentes plataformas de base de datos. Por último, muchas empresas de hospedaje web ofrecen una instalación gratuita de DotNetNuke junto con sus planes.

Completamente extensible y escalable. DNN es apto para una gran variedad de proyectos, desde el website más pequeño hasta el desarrollo corporativo más grande y complejo.

Webs de Internet o Intranet pueden ser completamente desarrolladas con las características intrínsecas de DotNetNuke. También pueden ser mejoradas con uno o varios de los cientos de módulos que extienden las funcionalidades de DotNetNuke.

Claramente licenciado bajo licencia BSD, el software puede ser completamente modificado, mejorado y adaptado a las necesidades personales o de empresa sin preocuparse por los aspectos legales.

LA APLICACIÓN SE REBAUTIZÓ COMO DOTNETNUKE, EN GRAN PARTE POR EL FRAMEWORK TECNOLÓGICO EN EL QUE ESTA BASADA .NET = DOTNET (EN INGLÉS) Y SE JUNTÓ CON "NUKE"

Evolución constante y testeo real permanente, incluso durante la realización del articulo presente, DNN evolucionó de versión desde la 5.1.0 a la 5.1.1, la naturaleza de DotNetNuke permite que los programadores y webmasters accedan, redistribuyan y modifiquen el código fuente, obteniendo en consecuencia una evolución constante del mismo.

Un gran equipo detrás de los "Core" de DotNetNuke hacen que las sugerencias de los usuarios finales se transformen rápidamente en mejoras en el software.

Eficiencia y Manejabilidad → DotNetNuke puede soportar múltiples portales desde una única instalación. Divide las opciones administrativas entre el nivel de host y el del portal individual, permitiendo gestionar cualquier número de sitios web, cada uno con su propia apariencia e identidad, todos desde una única cuenta de host.

Prioridad en la seguridad → Se ha puesto un especial énfasis en la validación, encriptación, detección y solventación de errores y amenazas potenciales.

Completamente personalizable → Se pueden realizar cambios en los portales a todos los niveles, desde ajustes básicos en las hojas de estilo como la tipografía, colores hasta en el aspecto completo del sitio web. Nuevas Skins y

WEBS DE INTERNET O INTRANET PUEDEN SER COMPLETAMENTE DESARROLLADAS CON LAS CARACTERÍSTICAS INTRÍNSECAS DE DOTNETNUKE. TAMBIÉN PUEDEN SER MEJORADAS CON UNO O VARIOS DE LOS CIENTOS DE MÓDULOS QUE EXTIENDEN LAS FUNCIONALIDADES DE DOTNETNUKE.

Containers pueden ser aplicados con facilidad sin repercusión en el contenido. Skin es una definición de "piel" para el sitio web, pudiendo cambiar su estética completamente con un clic de ratón. Un Container es una skin para el contenedor de un módulo.

Completamente Localizado → Construido con características multi-idioma, permite su uso, visualización y traducción en diferentes idiomas de una forma fácil.

Interfaz amigable → Un interfaz bien diseñado hace realmente fácil para un usuario el gestionar todos los aspectos del proyecto web, existiendo asistentes de sitio web, que junto al intuitivo interfaz de usuario nos permite una facilidad inusual para un sistema de estas características.

Gran soporte comunitario → Con una comunidad de más de 350.000 usuarios registrados y un gran numero de desarrolladores expertos en DotNetNuke, el servicio de hosting, soporte técnico y servicios de todo tipo siempre están a mano.

Pero, de donde viene DotNetNuke?

DotNetNuke, o también conocido como DNN para los amigos ;), viene de los principios de la tecnología .Net, surgiendo a raiz del lanzamiento, en enero del 2002, por parte de Microsoft del IBuySpy portal solution kit (IBS), un "starter kit", o a aplicación de ejemplo, que demostraba la aplicación de las mejores prácticas para la construcción de un portal dinámico y basado en base de datos. Debido a la calidad del código y a la aceptación del mismo por parte de la comunidad .Net, este se tomo como una implementación de referencia para desarrollar las aplicaciones ASP.Net.

El 24 de diciembre del 2002 Shaun Walter liberó una versión modificada del portal IBS original, a la que llamó IBuySpyWorkshop, con gran cantidad de mejoras respecto al original, como el soporte a múltiples portales, desde una única base de código. En las semanas siguientes a la versión "navideña" este fue descargado por miles y miles de usuarios de la comunidad de desarrolladores y fue tomada la decisión de evolucionar la aplicación a un proyecto de código abierto – un proyecto con una organización que gestione las versiones, su evolución y mejoras así como con una comunidad donde cualquiera pudiera acceder a las últimas versiones y características.

Después de un innombrable numero de releases y mejoras sobre la base de código original, la aplicación se rebautizó como DotNetNuke, en gran parte por el framework tecnológico en el que esta basada .Net = DotNet (en inglés) y se juntó con "Nuke" ya que es un termino ampliamente reconocido en la industria de los portales, ya que varios sistemas de portales llevan incluido este termino.

Instalación

Y bueno, para verlo adecuadamente nada mejor que instalarlo y jugar con ello no? Pues vamos a ver como podemos instalar la última versión de DotNetNuke y posteriormente veremos como crear alguna página y añadirle contenido.



LA CONFIGURACIÓN DE LAS PÁGINAS WEB CON DONTNETNUKE PERMITE DESARROLLAR PÁGINAS WEB CON MUCHA SOLVENCIA PUESTO QUE CUENTA CON UN ASISTENTE BASTANTE INTUITIVO QUE NOS PERMITIRÁ IR AVANZANDO EN EL PROCESO PASO A PASO.

En la reléase actual (DNN 5.1.1) tenemos varios paquetes disponibles: Source, Install, Upgrade y Starter Kit:

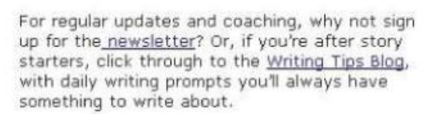
Source → Contiene todo el código fuente del framework, incluyendo las versiones ejecutables de todos los módulos. Para obtener el código de los módulos hay que realizarlo de forma separada.

Install (New Installation) → Contiene los ejecutable. Este paquete es principalmente para su instalación en producción partiendo de cero. No debemos utilizar esta versión para actualizar una instalación existente ya que hay otro paquete que se encarga de tal tarea.

Upgrade → Contiene los ejecutables y esta versión está preparada para actualizar una instalación previa.

VS Starter Kit → Contiene un ejecutable. Esta versión está diseñada para el desarrollo de software con Visual Studio, instalando varios tipos de proyectos de DNN que nos ayudarán sumamente a desarrollar soluciones personalizadas con el mínimo esfuerzo.









Como aquí somos todos desarrolladores, podemos realizar la instalación automatizada del "starter kit" o bien la del "Source". En cualquier caso la instalación del Source se asemeja más a la del paquete "install" que es el que deberemos utilizar para realizar el despliegue en un servidor web de producción.

Realizaremos por tanto la instalación del paquete "Source". Para ello primero deberemos descargarnos el software, DotNetNuke community edition, de http://www.dotnetnuke.com. Esta es en principio la única fuente de distribución existente del proyecto. Para ello deberemos registrarnos en la página web del proyecto e ir a la sección de descargas. (véase la imagen 1)



Para luego, descargarnos el archivo del paquete "Source", en este caso es "5.1.1 - Source Code (New Install + Source)", debiendo obtener el archivo: "DotNetNuke_Community_05.01.01_Source.zip".

Cabe destacar que DotNetNuke está preparado para ejecutarse en la versión "Express" de visual Studio, versión Open Source del popular entorno de desarrollo Visual Studio, que se puede obtener aquí: http://www.microsoft.com/express/

La instalación que aquí se comenta está realizada sobre Windows Vista aunque se dan indicaciones para realizarlo en otros sistemas. Si se siguen las indicaciones paso a paso finalizaremos estas con una instalación de DotNetNuke operativa ejecutandose sobre Windows Vista.

Descomprimir el paquete "Source" en un directorio vacío de tú máquina. En mi caso lo he instalado en c:\dnn511

Hacemos click con el boton derecho seleccionamos la opción propiedades. Desmarcamos la opción "Sólo lectura" y pulsamos aplicar.

Hacemos clic con el botón derecho del ratón sobre el directorio y seleccionamos la opción "Propiedades" y hacemos clic en la pestaña "Security". (Nota: en según qué sistemas operativos, la opción a hacer click será "Sharing and Security"). (si no tenemos la pestaña de seguridad, para activarla, debemos hacer clic en "Tools | Folder Options" seleccionar la pestaña "View", hacer scroll hasta debajo de todo y desactivar la opción de "Use simple file sharing")

Hacemos clic en el botón "Editar" y luego en "Agregar" y en el cuadro "Enter the object names to select" deberemos introducir el nombre la cuenta de sistema de ASP. La más común es que esta sea "ASPNET" para máquinas Windows Vista, Windows XP y Windows 2003 Server y "NETWORK SERVICE" para Windows Server 2003 en adelante. Bien, esto es así pero en realidad depende del servidor de Internet que tengamos instalado. Si tenemos IIS 6, deberemos utilizar "NETWORK SERVICE" y si es 5.x deberemos utilizar "ASPNET" sin tener en cuenta el sistema operativo. Introduciremos pues el nombre que corresponda.

Haremos clic en el botón "Check Names" y el nombre de usuario del sistema será validado y cualificado. Haremos clic en OK (véase imagen 2).



Seleccionamos la cuenta de usuario recién creada y le damos permisos a "Modify". No necesita tener "Full Control". Hacemos clic en el botón OK.

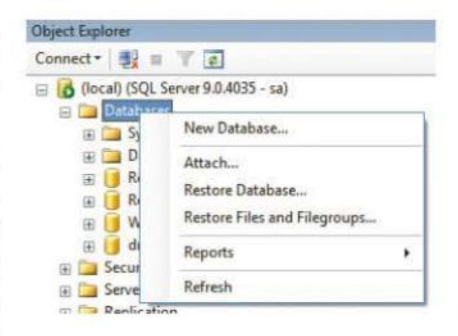
Dentro del directorio donde hemos descomprimido el paquete "Source" tendremos dos directorios, Library y Website. Dentro del directorio Website, que es la raíz del sitio web, en mi caso "C:\dnn511\Website" hacemos una copia del archivo release.config y lo renombramos a web.config. También copiamos el archivo \config\SiteUrls.config a la raiz del sitio web.

Crearemos la base de datos con la que trabajará nuestro portal, en mi caso acostumbro a trabajar con SQL Server, pero podríamos utilizar SQL Server Express, que es gratuito.

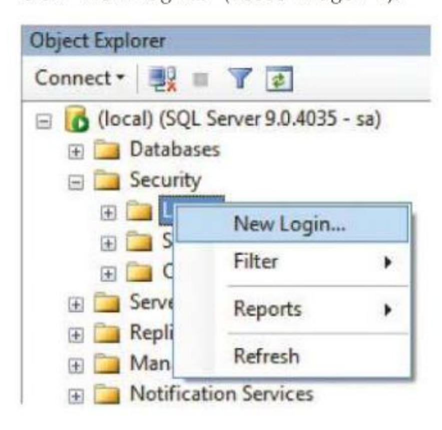
En cualquier caso quedaría extrapolar estos pasos a su sistema de gestión de base de datos preferido, siempre que esté soportado.

En cualquier caso, abrimos el SQL Server Management Studio y nos conectamos al servidor SQL Server en el que queramos tener la base de datos, en este caso, en local.

Hacemos clic derecho sobre Databases y hacemos clic izquierdo en la opción "New Database...". Le damos un nombre a la base de datos, dnn511 en nuestro caso y pulsamos el botón "OK" (véase imagen 3).

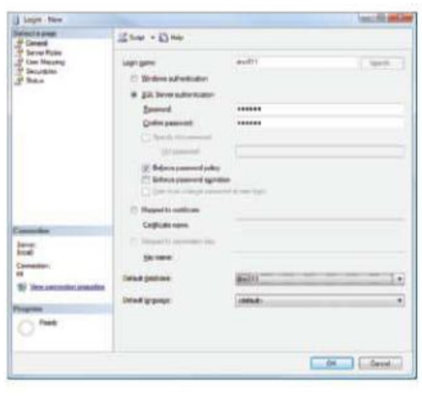


Creamos el usuario de la base de datos, desde el mismo SQL Server Management Studio, vamos a Security, Logins y hacemos clic derecho. Seleccionamos la opción "New Login..." (véase imagen 4).

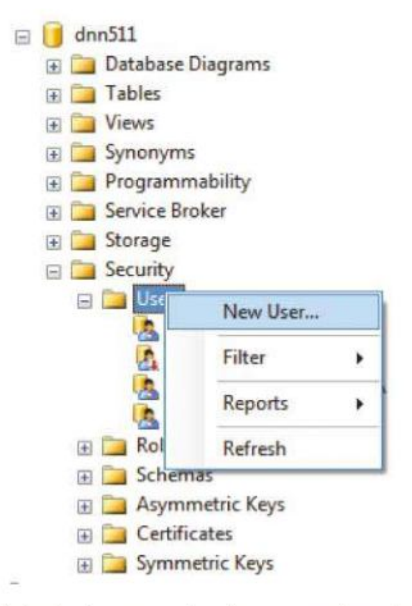




Una vez abierto el panel ponemos un nombre de usuario, por ejemplo, dnn511 y una contraseña. Desactivamos Enforce password expiration y seleccionamos la base de datos por defecto poniendo la que hemos creado recientemente (véase imagen 5).

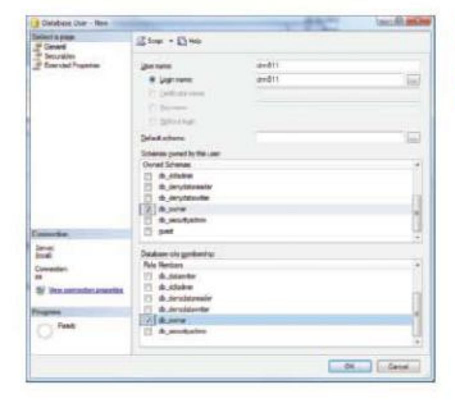


Posteriormente debemos crear este usuario en la base de datos (ahora lo hemos hecho para SQL Server). Para ello desplegaremos la base de datos, desplegaremos Security y haremos clic derecho en Users, haciendo clic izquierdo en "New User..." (véase imagen 6).



Introduciremos el mismo nombre de usuario previamente creado así como seleccionaremos el usuario de SQL Server haciendo clic en el boton "..." debajo del campo para el nombre.

Una vez hecho esto seleccionaremos "db_owner" en las dos listas, "Schemas owned by this user" y "Database role membership", tal y como se ve en la imagen 7.



CON DOTNETNUKE ESTAMOS EN DISPOSICIÓN DE PODER CREAR PÁGINAS WEB COMERCIALES, DE COMUNIDADES, INTRANETS CORPORATIVAS, EXTRANETS, PORTALES CMS Y APLICACIONES A MEDIDA. LA LIMITACIÓN ESTÁ EN LA IMAGINACIÓN DE CADA UNO.

Con ello ya hemos creado la base de datos y estamos listos para seguir. No nos preocuparemos por las tablas y demás elementos, DotNetNuke las creara automáticamente.

Abrimos el archivo web.config, ubicado en la raíz del sitio web, en un editor de texto o directamente en Visual Studio. Ahora vamos a las secciones de acceso a datos y comentaremos las dos claves SiteSqlServer de SQL Server 2005 Express, estas están al inicio, así que no será difícil hallarlas.

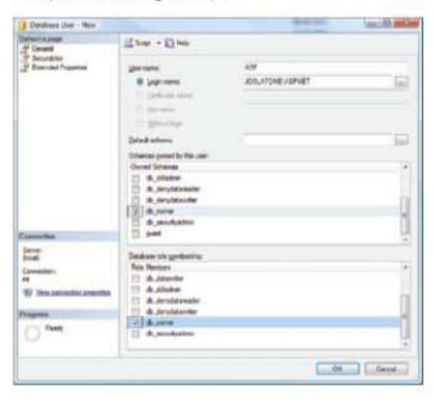
Seguido descomentamos las claves de SQL Server 2000/2005 y establecemos el valor de ambas como sigue: "Server=(local);Database=dnn511;uid =dnn511;pwd=dnn511;" (no hace falta decir que no se recomienda utilizar esta política de nombres y mucho menos de contraseñas en un entorno de producción..).

En Database ponemos el nombre de la base de datos, en uid, ponemos el nombre de usuario y en pwd el password que hayamos puesto en SQL Server para el usuario en cuestión. Nos aseguramos de que ambas claves SiteSqlServer tienen la misma cadena de conexión, grabamos y cerramos el fichero web.config. No modificamos nada más.

Nota: En la cadena de conexión, si no funciona, probad a substituir (local) por el nombre del servidor de base de datos o nombre de equipo/servidor de base de datos.

Ahora vamos a dar permisos a la cuenta de sistema de ASP para que pueda generar la base de datos. Abrimos el SQL Server Management Studio y desplegamos la sección "Security" y tal como hemos hecho en el punto 8, añadimos la cuenta de sistema de ASP (ASPNET o Network Authority), según la versión del IIS, recordemos. Le damos el acceso por defecto a la base de datos "master".

Ahora le damos permisos a esta cuenta para que tenga control total sobre nuestra base de datos, de forma idéntica al punto 9, creamos el usuario "ASP" y le otorgamos permisos de db_owner. Hacemos clic en OK y Cerramos el SQL Server Management Studio. Ahora sólo nos queda configurar el servidor de Internet IIS (véase imagen 8).



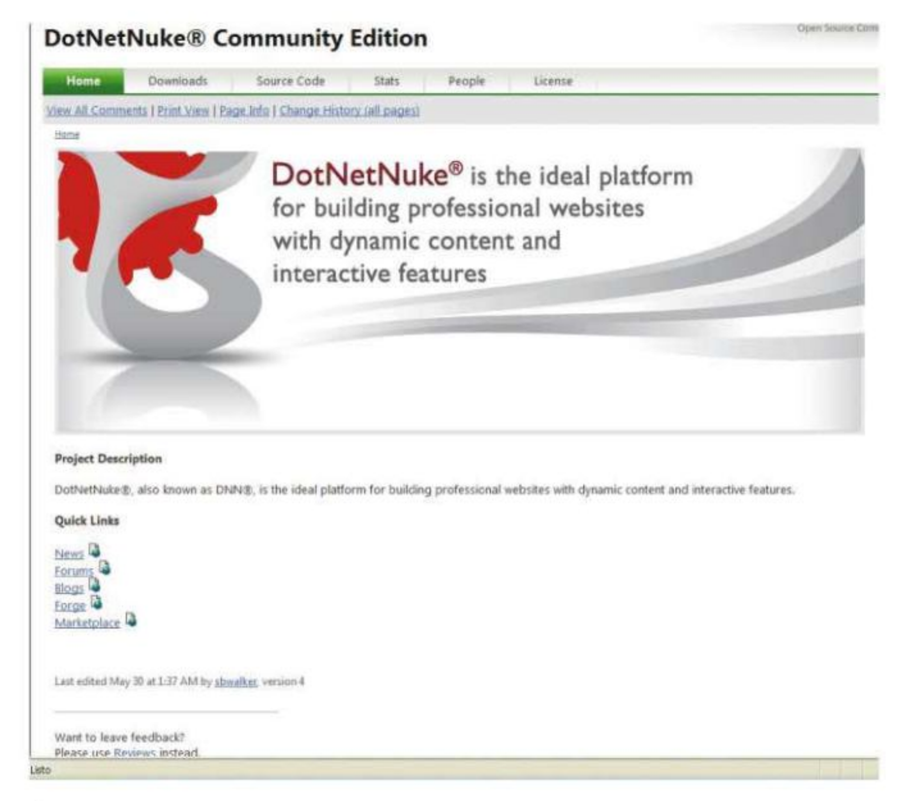
Abrimos el administrador de IIS (Internet Information Services) y añadimos un nuevo directorio virtual en la raíz del website por defecto. Le llamamos "dnn511" por coherencia y hacemos que apunte al directorio raiz del website, en mi caso "C:\dnn511\Website". Verificamos que "Read" y "Run Scripts" estén seleccionados y aceptamos el resto de selecciones por defecto.

Hacemos clic derecho sobre el nuevo sitio web en IIS y seleccionamos "Properties". Seleccionamos la pestaña ASP.Net y nos aseguramos de que la versión de .Net asociada sea la correcta 2.0, en nuestro caso.

Debemos asociar la página por defecto a nuestro directorio virtual, haciendo clic derecho abrimos la ventana de Properties y nos vamos a la pestaña Documents. Allí pulsamos el botón "Add..." y añadimos "default.aspx" y lo subimos arriba de todo, para que sea la primer página en cargar.

La configuración ha finalizado. Si no hay ningún problema con el equipo y componentes, abriendo un navegador y yendo a http://localhost/dnn437 deberia iniciar el proceso de instalación de DotNetNuke. Una vez la instalación ha concluido, tendremos un enlace al fondo de la página que nos llevará al nuevo portal. La instalación sólo se ejecutará una vez.

En el proceso de instalación se nos presentará la evolución de la instalación como se puede apreciar en la siguiente pantalla, en la que se pregunta sobre el modo de instalación y el lenguaje de la misma.





Seguidamente pulsamos Siguiente y veremos el progreso de la instalación que hayamos seleccionado, seleccionaremos el "Típico". La siguiente pantalla que se nos mostrará al pulsar "Siguiente" será la de validación de permisos de ficheros:



En esta deberemos hacer click en "Prueba de permisos", que validará los permisos necesarios de acceso y nos indicará en pantalla si las pruebas finalizan con éxito o no. Seguido, pulsaremos siguiente para acceder a la pantalla de "configuración de la conexión de la base de datos", que nos permite hacer lo mismo que hemos hecho para la cadena de conexión "a mano", pero de una forma más asistida:

Aquí podremos probar la conexión y reconfigurarla según consideremos oportuno. Seguido podemos ver el proceso de creación de la base de datos:

Seguidamente nos pedirá configurar el usuario Host, que es el que posee los mayores permisos, el superusuario de todo el conjunto de portales que maneje la instalación actual de DotNetNuke. Tw wambién nos permitirá configurar el servidor SMTP que tengamos contratado y probar su buen funcionamiento. En este caso aceptamos los valores por defecto y añadimos una contraseña y una dirección de correo valida. La siguiente pagina del asistente nos permite configurar el administrador del portal, es decir de uno de los portales que tengamos en la instalación de DotNetNuke - recordemonos que era multiportal ;) - y le podremos indicar el portal que nos va a crear por defecto en la instalación, le pondremos "arroba" y pulsaremos siguiente.

Seguido nos indicara - si todo ha ido bien, sera muy seguro que esto sea así - que la instalación ha finalizado con éxito:



Si hacemos clic en el enlace "Proceso finalizado (ir a la web)", nos llevara a nuestra flamante nuevo portal web, como podemos ver en la siguiente imagen 15.



La siguiente vez que accedamos a esta dirección (http://localhost/dnn511/) se nos visualizará el la página principal del sitio web por defecto de DotNetNuke, en su última versión, como nos gusta a la mayoría @.

Solo queda felicitaros, si habéis llegado hasta aquí, habréis instalado y configurado vuestro portal web DotNetNuke con éxito.

José Luis Latorre
http://www.bcndev.net

En el mundo de la criptografía, como ocurre en tantos otros ámbitos, todo termina guardando cierta relación. No tiene sentido concebir la infraestructura de clave pública (PKI) sin involucrar en ella a la criptografía simétrica, la criptografía asimétrica, los algoritmos de resumen hash, y los algoritmos de autenticación MAC. Por supuesto, nosotros no íbamos a ser una excepción a esto, por lo que en nuestra nueva cripto-criatura (jWadalPasswd), vamos a tener que echar mano de más "criptocosas" para poder continuar desarrollando nuestro sistema criptográfico.



jWadalPasswd (II)

Bienenidos seáis todos una vez más, queridos lectores. Contra viento, marea, y demás vicisitudes pseudoaleatorias, el Curso de Java Útil continúa ofreciéndoos entretenimiento que llevar a vuestros ociosos compiladores. El mes pasado iniciamos una nueva etapa en el presente curso, al comenzar a desarrollar una nueva aplicación llamada jWadalPasswd.

¿Dónde estábamos?

En la entrega anterior, y tras una breve introducción teórica a los criptosistemas informáticos actuales, comenzamos a desarrollar el motor criptográfico de nuestra nueva criatura. En concreto, codificamos un par de métodos en la clase Cipher para cifrar y descifrar información respectivamente, mediante el algoritmo criptográfico simétrico AES, y sirviéndonos para ello de la API criptográfica libre Bouncy Castle (http://www.bouncycastle.org/). Finalmente, comprobamos el correcto funcionamiento del código, e hicimos alguna "trastada" para ver por dónde rompía.

Eso sí, que conste que no me olvido de los "deberes" que dejé. En una de las últimas pruebas que hicimos con el código para probar los métodos criptográficos, redujimos la longitud de la clave en un carácter, obteniendo el siguiente error:

```
Exception in thread "main" java.
lang.IllegalArgumentException: Key
length not 128/192/256 bits.
  at org.bouncycastle.crypto.engi-
nes.AESEngine.generateWorkingKey(U
nknown Source)
  at org.bouncycastle.crypto.engi-
nes.AESEngine.init(Unknown Source)
  at org.bouncycastle.crypto.
modes.CBCBlockCipher.init(Unknown
Source)
  at org.bouncycastle.crypto.
paddings.PaddedBufferedBlockCi-
pher.init(Unknown Source)
  at jwadalpasswd.cripto.Cipher.
cifrar(Cipher.java:45)
  at jwadalpasswd.Main.main(Main.
java:29)
Java Result: 1
```

Esta excepción (del tipo "IllegalArgumentException") nos está indicando que la longitud de la clave no es válida. Al parecer, la clave a utilizar para ejecutar el proceso de cifrado del algoritmo AES debe tener un tamaño determinado: 128, 192 ó 256 bits. Pero, por otro lado, y desde el punto de vista del usuario del programa, lo que tiene sentido es utilizar una cadena de texto como contraseña que proteja los datos cifrados.

Recapitulando: necesitamos que, dada una entrada con una cadena de texto de longitud arbitraria, generemos una salida con una cadena de información (no necesariamente de texto) de un tamaño fijo. ¿Os suena de algo? ¡Bingo!

Hashes redux

Como la mayoría de vosotros habréis pensado -o eso espero-, la solución pasa por acudir a unos "viejos amigos" de nuestra primera aplicación en el presente curso: los hashes criptográficos. Si echamos la vista atrás, concretamente al segundo artículo

del presente curso (publicado en el número 131 de @RROBA), podremos rescatar las cuatro propiedades que enunciamos para las funciones criptográficas de tipo hash. Una de ellas, que conocemos como la propiedad de "compresión", dice que el tamaño de la salida del algoritmo es fijo. Creo que recordaréis bastante bien cómo funcionaban esta clase de funciones, pues jWadalHash se dedicaba básicamente a calcularlas utilizando distintos algoritmos.

Sea como fuere, nuevamente necesitamos recurrir a nuestras queridas funciones hash para solventar un pequeño escollo en el desarrollo de jWadalPasswd. La idea es utilizar la contraseña -una cadena de texto de tamaño arbitrario- como entrada para la función hash, la cual generará una cadena de salida de tamaño fijo, que será a su vez utilizada como clave para cifrar la información mediante AES.

Llegados a este punto, debemos decidir qué algoritmo de hash utilizaremos. Nos sirve cualquiera que genere salidas de 128, 192 ó 256 bits; si bien, en aras de la simplicidad y la facilidad de cómputo, nos quedaremos con la más estándar: MD5. Esta función, que se encontraba entre las soportadas por jWadalHash, genera salidas de 128 bits de longitud, por lo que cumple con nuestras expectativas.

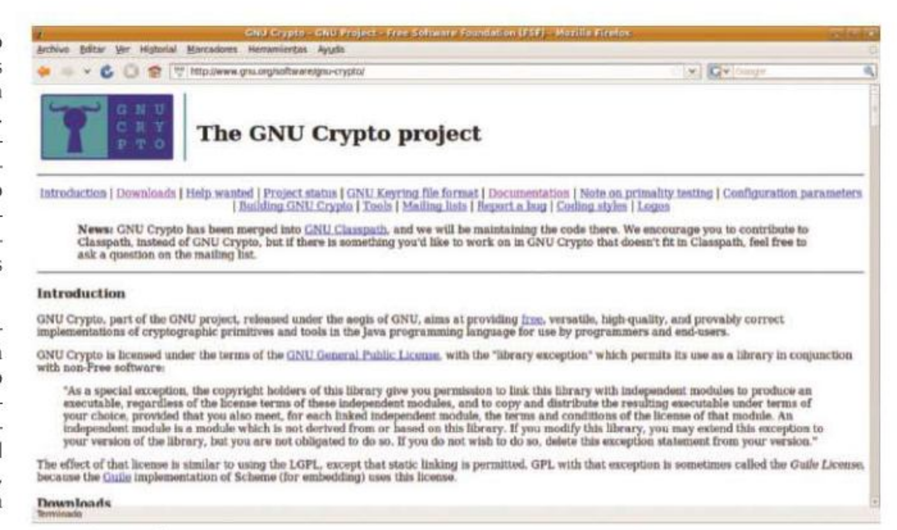
Sin embargo, y ya que estamos aquí para aprender cosas nuevas e interesantes, no vamos a utilizar directamente el código que generamos para jWadalHash. Si recordáis, para implementar el motor criptográfico en su día, nos basamos en la API GNU Crypto (http://www.gnu.org/software/gnu-crypto/). En esta ocasión, no obstante, estamos utilizando la API de Bouncy Castle (http://www.bouncycastle.org/), y no tiene sentido importar infinidad de bibliotecas de código de forma gratuita, pues aumentará el peso del paquete final del programa. Por tanto, vamos a volver a implementar el cálculo del hash MD5 mediante la API de Bouncy Castle.

Hashes en Bouncy Castle

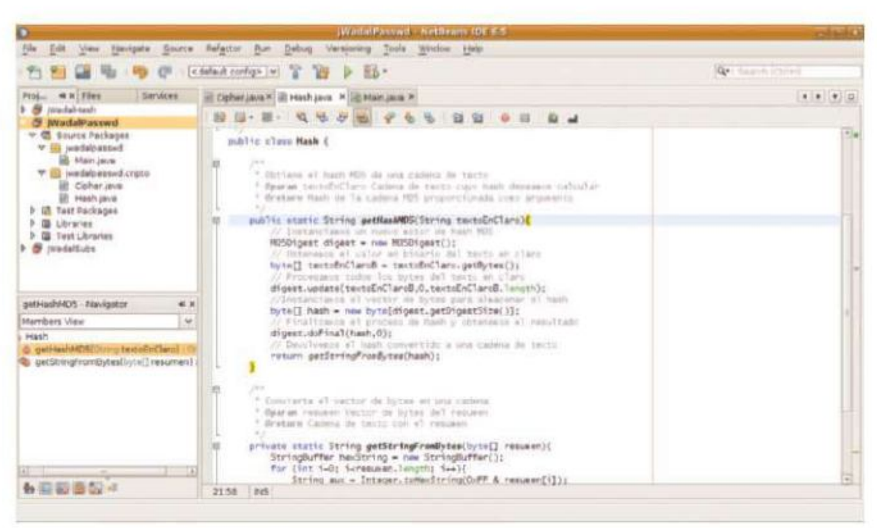
Lo primero que haremos es crear una nueva clase llamada "Hash.java" en el paquete de código "jwadalpasswd.cripto". En dicha clase crearemos un método público y estático llamado "getHashMD5", que recibirá una cadena con el texto en claro cuyo hash queremos calcular, y devolverá una cadena de texto con la representación en hexadecimal del resultado de la función hash MD5.

```
public static String
getHashMD5(String textoEnClaro){
}
```

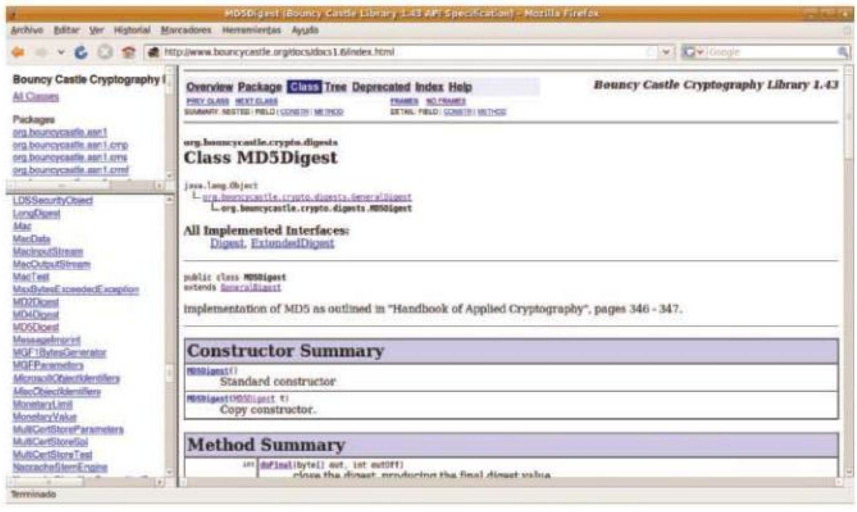
Una vez metidos en la implementación de dicho método, lo primero será instanciar el motor criptográfico del algoritmo de Hash



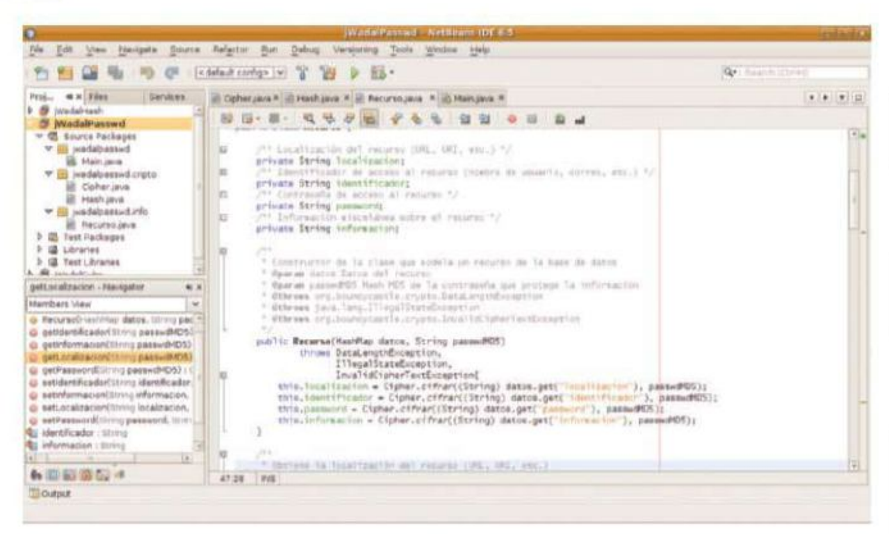
API criptográfica GNU Crypto



Implementación de MD5 en Bouncy Castle.



La clase MD5Digest de Bouncy Castle



La clase MD5Digest de Bouncy Castle

MD5, usando para ello la clase MD5Digest de Bouncy Castle (http://www.bouncycastle.org/docs/docs1.6/org/bouncycastle/crypto/digests/MD5Digest.html), que se encuentra en el paquete "org.bouncycastle.crypto.digests":

```
MD5Digest digest = new MD5Di-
gest();
```

Inmediatamente después, obtendremos la representación binaria de la entrada en un vector de bytes, al igual que hacíamos en los métodos para cifrar y descifrar información:

```
byte[] textoEnClaroB = textoEnCla-
ro.getBytes();
```

A continuación, invocaremos al método "update" de la clase GeneralDigest (http://www.bouncycastle.org/docs/docs1.6/org/bouncycastle/crypto/digests/GeneralDigest.html#update(byte[],%20int,%20int)), que se encargará de procesar todos los bytes de la entrada:

```
digest.update(textoEnClaroB,0,text
oEnClaroB.length);
```

Instanciaremos un vector de bytes para almacenar el resultado de la función hash...

```
byte[] hash = new byte[digest.
getDigestSize()];
```

...y finalizaremos el cómputo invocando al método "doFinal" de la clase MD5Digest (http://www.bouncycastle.org/docs/docs1.6/org/bouncycastle/crypto/digests/MD5Digest.html#doFinal(byte[],%20int)), para generar el valor final y reiniciar el motor MD5.

```
digest.doFinal(hash,0);
```

Por último, devolveremos el valor del resultado convertido a una cadena de texto:

```
return getStringFromBytes(hash);
```

El método completo tendrá el siguiente aspecto:

```
/**
 * Obtiene el hash MD5 de una ca-
dena de texto
 * @param textoEnClaro Cadena de
texto cuyo hash deseamos calcular
 * @return Hash de la cadena MD5
proporcionada como argumento
 */
public static String
getHashMD5(String textoEnClaro){
  // Instanciamos un nuevo motor
de hash MD5
  MD5Digest digest = new MD5Digest();
  // Obtenemos el valor en binario
del texto en claro
  byte[] textoEnClaroB = textoEn-
Claro.getBytes();
  // Procesamos todos los bytes
del texto en claro
  digest.update(textoEnClaroB,0,te
xtoEnClaroB.length);
  //Instanciamos el vector de
bytes para almacenar el hash
  byte[] hash = new byte[digest.
getDigestSize()];
  // Finalizamos el proceso de
hash y obtenemos el resultado
  digest.doFinal(hash,0);
  // Devolvemos el hash convertido
a una cadena de texto
  return getStringFromBytes(hash);
}
```

Como habréis intuido, será necesario copiar el código del método "getStringFromBytes" que impementamos para jWadalHash:

```
/**
 * Convierte el vector de bytes en
una cadena
 * @param resumen Vector de bytes
del resumen
 * @return Cadena de texto con el
resumen
 */
private static String getStringFro
mBytes(byte[] resumen){
  StringBuffer hexString = new
StringBuffer();
  for (int i=0; i<resumen.length;
```



```
i++){
   String aux = Integer.
toHexString(0xFF & resumen[i]);
   if (aux.length() < 2){
   aux = "0" + aux;
   }
   hexString.append(aux);
   }
   return hexString.toString();
}
```

Nuevas pruebas de cifrado

Ahora, y con el nuevo método para calcular hashes en MD5, podemos modificar el código de prueba de la clase "Main" para que calcule la contraseña como el hash de un texto de entrada:

```
/**
 * @param args the command line
arguments
 */
public static void main(String[]
args)
   throws DataLengthException,
   IllegalStateException,
   InvalidCipherTextException {
   String textoEnClaro = "prueba";
   String clave = "contraseña";
   String claveHash = Hash.
getHashMD5(clave);
   System.out.println();
   System.out.println("Usando la
clave \"" + clave + "\" (" + cla-
veHash + ")");
   System.out.println();
   System.out.println("Cifrando: "
+ textoEnClaro);
   String criptograma = Cipher.
cifrar(textoEnClaro,claveHash);
   System.out.println("Criptograma:
" + criptograma);
   System.out.println();
   System.out.println("Descifrando:
" + criptograma);
   String descifrado = Cipher.
descifrar(criptograma,claveHash);
   System.out.println("Texto desci-
frado: " + descifrado);
   System.out.println();
}
```

La salida que obtendremos al ejecutar dicho código será la siguiente:

```
Usando la clave "contraseña"
(4c882dcb24bcb1bc225391a602feca7c)

Cifrando: prueba
Criptograma:
IIKn7K+D5bej8TEkofGrNw==

Descifrando:
IIKn7K+D5bej8TEkofGrNw==
Texto descifrado: prueba
```

Si cambiamos la contraseña por, por ejemplo, la cadena "@RROBA", obtendremos esta otra salida:

```
Usando la clave "@RROBA" (ffa-
6c38ab4399b07b0588a891b0353c7)

Cifrando: prueba
Criptograma: gOy0m/xxbaL-
z9UWCZ1GmpA==

Descifrando: gOy0m/xxbaL-
z9UWCZ1GmpA==
Texto descifrado: prueba
```

Parece que, ahora sí, podemos utilizar cualquier cadena de texto para cifrar la información.

Modelando los secretos

Una vez finalizado el motor criptográfico de nuestra nueva aplicación, nos encontramos en disposición de modelar los tipos de datos que soportarán la información contenida en la misma. Concretamente, vamos a comenzar modelando el tipo de datos para un recurso, esto es, una entrada en nuestra base de datos. Este recurso contendrá información sobre la localización del mismo (por ejemplo, una dirección web), un identificador de usuario, una contraseña de acceso (motivación principal de nuestra aplicación), así como otros datos que pudieran resultar interesantes.

Podríamos codificar esta información mediante una lista de cadenas en una clase más genérica, si bien en tal caso tendríamos un problema de escalabilidad: añadir un elemento en la información que almacenamos de cada recurso supondría, a la postre, modificar el atributo que lo almacena, así como los métodos que acceden a dicho atributo. Modelando la información como una clase independiente, obtenemos la capacidad de incrementar la información almacenada simplemente añadiendo un atributo, así como los métodos "getter" y "setter" pertinentes.

Vamos a crear una nueva clase llamada "Recurso.java", que estará contenida en un nuevo paquete de código llamado "jwadalpasswd.info". Una vez creada, crearemos los atributos pertinentes para almacenar la información anteriormente enunciada:

```
/** Localización del recurso (URL,
URI, etc.) */
private String localizacion;
/** Identificador de acceso al re-
curso (nombre de usuario, correo,
etc.) */
private String identificador;
/** Contraseña de acceso al recur-
so */
private String password;
/** Información miscelánea sobre
el recurso */
private String informacion;
```

El siguiente paso lógico es generar el constructor de la clase, que debe recibir dichos datos, así como la clave de cifrado que se usará para almacenarlos en memoria. Es importante tratar de que la información en claro esté almacenada en el menor número posible de sitios. La interfaz del constructor será como podéis ver a continuación:

```
public Recurso(HashMap datos,
String passwdMD5){
}
```

Puede que a alguno de vosotros le llame la atención la "poca" cantidad de parámetros que está recibiendo el constructor, ya que la clase está almacenando la información en cuatro atributos diferentes. Perfectamente podríamos haber hecho que el constructor recibiera cinco parámetros de tipo String: uno por cada uno de los atributos, y uno más con la contraseña de cifrado. Sin embargo, esta solución habría sido poco elegante, pues tendríamos un método constructor que recibe un número muy elevado de parámetros del mismo tipo, algo que podemos solucionar utilizando un mapa de datos.

HashMap

Para implementar dicha solución, vamos a utilizar una estructura de datos conocida como HashMap (http://java.sun.com/javase/6/docs/api/java/util/HashMap.html), y que contiene parejas de datos "clave:valor", donde la clave es el objeto que sirve para indexar (es decir, almacenar y recuperar) la información contenida en el objeto que contiene el valor.

Así, para añadir un nuevo objeto al HashMap, usaremos el método "put" (http://java.sun.com/javase/6/docs/api/java/util/HashMap.html#put(K,%20V)); mientras que pare recuperar objetos utilizaremos el método "get" (http://java.sun.com/javase/6/docs/api/java/util/HashMap.html#get(java.lang.Object)). En nuestro caso, la clave será una cadena con el nombre del atributo almacenado en el valor. De esta forma, implementaremos el constructor de la siguiente forma:

```
/**
 * Constructor de la clase que mo-
dela un recurso de la base de datos
 * @param datos Datos del recurso
 * @param passwdMD5 Hash MD5 de la
contraseña que protege la infor-
mación
 * @throws org.bouncycastle.cryp-
to.DataLengthException
```

```
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public Recurso(HashMap datos,
String passwdMD5)
  throws DataLengthException,
  IllegalStateException,
  InvalidCipherTextException{
  String tmp = null;
  tmp = (String) datos.
get("localizacion");
  this.localizacion = Cipher.
cifrar(tmp, passwdMD5);
  tmp = (String) datos.
get("identificador");
  this.identificador = Cipher.
cifrar(tmp, passwdMD5);
  tmp = (String) datos.
get("password");
  this.password = Cipher.
cifrar(tmp, passwdMD5);
  tmp = (String) datos.
get("informacion");
  this.informacion = Cipher.
cifrar(tmp, passwdMD5);
}
```

Como podéis ver, para cada valor contenido en el HashMap, necesitamos obtener el objeto y realizar una conversión cast a su tipo de datos original. Sin embargo, y para evitar estar repitiendo tanto el código, podemos comprimir un poco la sintaxis, realizando dos pasos en uno:

```
/**
 * Constructor de la clase que
modela un recurso de la base de
datos
 * @param datos Datos del recurso
 * @param passwdMD5 Hash MD5 de la
contraseña que protege la informa-
ción
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public Recurso(HashMap datos,
String passwdMD5)
  throws DataLengthException,
  IllegalStateException,
  InvalidCipherTextException{
  this.localizacion = Ci-
pher.cifrar((String) datos.
get("localizacion"), passwdMD5);
  this.identificador = Ci-
pher.cifrar((String) datos.
get("identificador"), passwdMD5);
  this.password = Ci-
pher.cifrar((String) datos.
get("password"), passwdMD5);
  this.informacion = Ci-
pher.cifrar((String) datos.
get("informacion"), passwdMD5);
}
```

Por otro lado, habréis notado que estamos arrojando las excepciones criptográficas a la instancia llamante. Esto es así porque, en caso de error en el proceso de cifrado, querremos que dicha información llegue a la interfaz de usuario, para poder informar de forma adecuada del tipo de error.

El siguiente paso, y para cerrar la implementación de esta clase, consistirá en crear los métodos "getter" y "setter" para cada atributo de la misma:

```
/**
 * Obtiene la localización del re-
curso (URL, URI, etc.)
 * @param passwdMD5 Hash de la
contraseña MD5 que protege la in-
formación
 * @return Localización del recur-
so (URL, URI, etc.)
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public String
getLocalizacion(String passwdMD5)
  throws DataLengthException,
  IllegalStateException,
  InvalidCipherTextException{
  return Cipher.descifrar(this.
localizacion, passwdMD5);
}

/**
 * Almacena la localización del
recurso (URL, URI, etc.)
 * @param localizacion Localiza-
ción del recurso (URL, URI, etc.)
 * @param passwdMD5 Hash de la
contraseña MD5 que protege la in-
formación
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public void setLocalizacion(String
localizacion, String passwdMD5)
  throws DataLengthException,
  IllegalStateException,
  InvalidCipherTextException{
  this.localizacion = Cipher.
cifrar(localizacion, passwdMD5);
}

/**
 * Obtiene el identificador de ac-
ceso al recurso (nombre de usua-
rio, correo, etc.)
 * @param passwdMD5 Hash de la
contraseña MD5 que protege la in-
formación
 * @return Identificador de acce-
so al recurso (nombre de usuario,
correo, etc.)
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public String
getIdentificador(String passwdMD5)
  throws DataLengthException,
  IllegalStateException,
  InvalidCipherTextException{
  return Cipher.descifrar(this.
identificador, passwdMD5);
}

/**
 * Almacena el identificador de ac-
ceso al recurso (nombre de usua-
rio, correo, etc.)
 * @param identificador Identifica-
dor de acceso al recurso (nombre
de usuario, correo, etc.)
 * @param passwdMD5 Hash de la
contraseña MD5 que protege la in-
formación
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public void setIdentificador(String
identificador, String passwdMD5)
  throws DataLengthException,
  IllegalStateException,
  InvalidCipherTextException{
  this.identificador = Cipher.
cifrar(identificador, passwdMD5);
}

/**
 * Obtiene la contraseña de acceso
al recurso
 * @param passwdMD5 Hash MD5 de la
contraseña que protege la informa-
ción
 * @return Contraseña de acceso al
recurso
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public String getPassword(String
passwdMD5)
  throws DataLengthException,
  IllegalStateException,
```

```
    InvalidCipherTextException{
    return Cipher.descifrar(this.
password, passwdMD5);
}

/**
 * Almacena la contraseña de acce-
so al recurso
 * @param password Contraseña de
acceso al recurso
 * @param passwdMD5 Hash MD5 de la
contraseña que protege la informa-
ción
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public void setPassword(String
password, String passwdMD5)
    throws DataLengthException,
    IllegalStateException,
    InvalidCipherTextException{
    this.password = Cipher.
cifrar(password, passwdMD5);
}

/**
 * Obtiene la información misce1á-
nea sobre el recurso
 * @param passwdMD5 Hash MD5 de la
contraseña que protege la informa-
ción
 * @return Información miscelánea
sobre el recurso
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public String
getInformacion(String passwdMD5)
    throws DataLengthException,
    IllegalStateException,
    InvalidCipherTextException{
    return Cipher.descifrar(this.
informacion, passwdMD5);
}

/**
 * Almacena la información misce-
lánea sobre el recurso
 * @param informacion Información
miscelánea sobre el recurso
 * @param passwdMD5
 * @throws org.bouncycastle.cryp-
to.DataLengthException
 * @throws java.lang.IllegalState-
Exception
 * @throws org.bouncycastle.cryp-
to.InvalidCipherTextException
 */
public void setInformacion(String
informacion, String passwdMD5)
    throws DataLengthException,
    IllegalStateException,
    InvalidCipherTextException{
    this.informacion = Cipher.
cifrar(informacion, passwdMD5);
}
```

El mes que viene

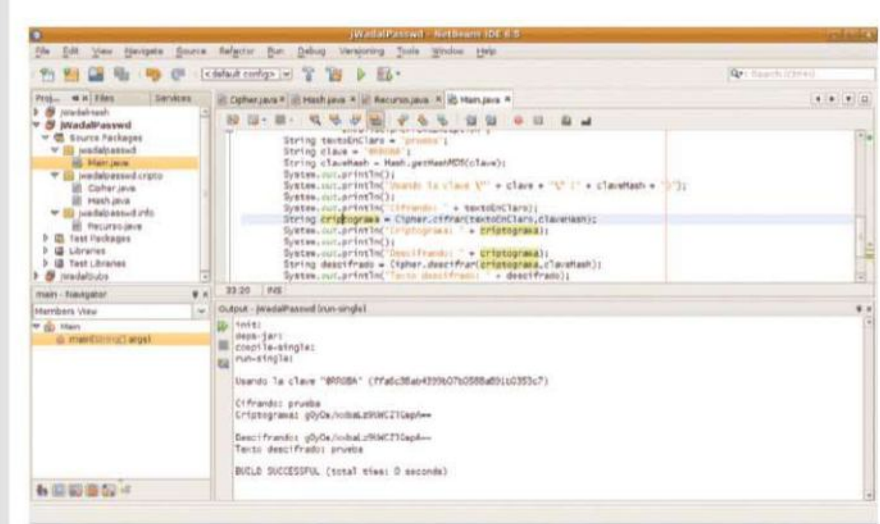
Este mes hemos implementado un mecanismo que, gracias al uso de las funciones criptográficas de tipo hash, nos permite utilizar los mecanismos de cifrado y descifrado de la API de Bouncy Castle (con tamaños de clave fijos) mediante cualquier contraseña proporcionada por el usuario. Además, hemos creado una clase que modela el tipo de datos de un recurso, y que servirá de base para la información que almacenaremos en la base de datos de nuestra aplicación.

El mes que viene continuaremos desarrollando nuestra aplicación, incluyendo información para modelar distintos usuarios en la aplicación, así como validar la contraseña de cifrado contra información almacenada de forma persistente. En este caso, no podemos almacenar el hash de la contraseña, pues supondría dar acceso instantáneo a toda la información cifrada con dicho hash. ¿Se os ocurre alguna solución? Nuevamente, ya conocéis la respuesta a este problema, así que podéis pensar en ello hasta la siguiente entrega.

Como cada mes, me permito recordaros que disponéis del código fuente del curso en mi blog personal, y que podéis enviar dudas o sugerencias acerca del curso a mi correo electrónico.

¡Hasta el mes que viene!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/



Probando nuestro mecanismo de cifrado



El universo blog en el iPhone

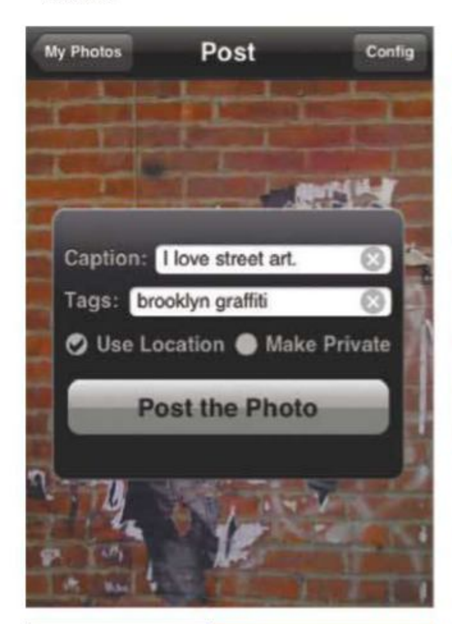
Si dispones de un iPhone y además tienes un blog o eres seguidor de alguno, a continuación te presentamos un sinfín de posibilidades para que puedas actualizar tu sitio web al instante o puedas ver estos cambios en la pantalla de tu móvil.



Los usuarios de los blogs están de suerte ya que tienen a su disposición una herramienta que permite volcar sus impresiones a la web sin tener que esperar a ponerse delante del ordenador: el iPhone. Gracias al amplio catálogo de aplicaciones existente en la actualidad, quien tenga un blog puede crear y editar posts, administrar comentarios y configurar preferencias, subir fotos, etc., en el momento o en cualquier sitio y a cualquier hora. Por su parte, los lectores podrán consultar sus páginas favoritas cuando lo deseen. Lo más fácil a la hora de instalar una de estas aplicaciones en el iPhone es emplear el mismo servidor de blog que se usa normalmente. Pero, al ser una oferta muy extensa, también se puede disponer de programas que permiten escribir en varios sitios webs o realizar un uso más confeccionado. Estos son alguno de ellos:

CLOWDY PHOTO BLOGGER

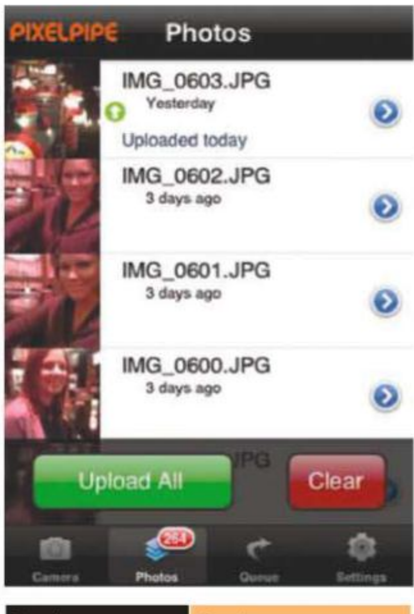
Si tienes un blog en Clowdy puedes darte de alta en este servicio desde el iPhone. Se pueden subir imágenes al servidor tanto de la cámara como de la biblioteca de fotos y deja acceder a los álbumes de otras personas que también lo usan.



Precio	Gratis
Idioma	Inglés
Compatibilidad	iPhone e iPod Touch

PIXELPIPE

Tiene configurados varios servicios como el popular Blogger de Google o TypePad, por lo que se puede enviar imágenes a cualquiera de ellos, según los que el usuario configure. La búsqueda e identificación de las imágenes se consigue a través de un pequeño texto y una serie de etiquetas.



Precio	Gratis
Idioma	Inglés
Compatibilidad	iPhone

LIFECAST

Es un editor de blogs que utiliza servicios como Blogger de Google y Tumbar, posibilitando la gestión de varios blogs, la publicación de entradas en cada uno de ellos, etc., con la finalidad de compartir textos, música, vídeos... Se pueden subir fotografías del Iphone al blog como una entrada aparte, pero en este caso no es posible añadir un texto a la imagen, sólo el título y la localización.



Precio	Gratis
Idioma	Español
Compatibilidad	iPhone e iPod Touch

BLOGWRITER

Combina funciones de edición de blog con otros servicios. Se trata de un lector de noticias RSS que permite la suscripción y lectura de los artículos escritos en otros blogs y también de las noticias publicadas en múltiples medios de comunicación.

Funciona con cualquier servidor que soporte el protocolo MetaWeblog, pero no permite hacer fotografías directamente, aunque sí añadirlas desde el álbum de fotos.





Precio	1,59 euros
Idioma	Inglés
Compatibilidad	iPhone e iPod Touch

BLOGWRITER (LITE)

Para probar la versión anterior de forma gratuita se puede descargar la adaptación Lite. Este es un programa completo pero que cuenta con características y funcionalidades que están restringidas, aunque no todas.

En este caso, limita las opciones de texto y únicamente permite la suscripción a dos RSS. Por lo demás, la funcionalidad está completa.

Precio	Gratis
Idioma	Inglés
Compatibilidad	iPhone e iPod Touch



BLOGPRESS

Esta aplicación es capaz de manejar los servidores de blogs Blogger, Msn Live Spaces, Movable Type, WordPress y TypePad, entre otros. Además, es el único programa que permite añadir fotos a un artículo publicado en Blogger.

Por otra parte, su editor de textos facilita que la integración de las imágenes en su texto correspondiente resulte muy intuitiva. De esta forma se hace posible el envío de un mismo post a más de un blog, si fuera necesario.

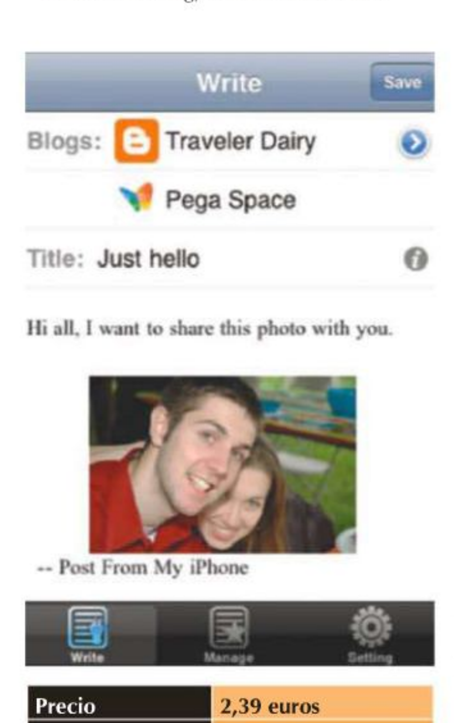
BLOG WITH IBLOGGER

Ayuda a gestionar varios blogs simultáneamente, incluyendo los más conocidos: Blogger, WordPress, TypePad y muchos más. Además, no sólo permite crear nuevas entradas en el blog, sino que al conectarse al servidor se descarga la lista de entradas que hay, aunque no hayan sido creadas con este programa, y así visualizarlas, editarlas y volverlas a subir, una vez modificadas. Dispone de geolocalización y se puede insertar hiperenlaces y etiquetas e imágenes en los blogs, si el servidor configurado lo permite, para clasificar el artículo publicado.

CELLSPIN

Con esta aplicación, los usuarios pueden capturar textos, fotos y audio desde el iPhone con un solo click.

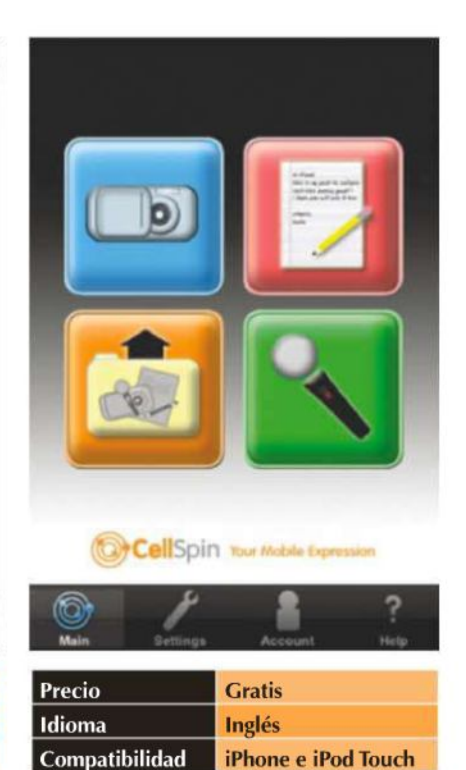
Asimismo, y de manera simultanea publicarlo fácilmente en diferentes sitios: en sus propios servidores o en otros externos, con toda la facilidad del cortar y pegar, o lo que es lo mismo con un único clic.



Precio	2,39 euros
Idioma	Español
Compatibilidad	iPhone e iPod Touch



Precio	7,99 euros
Idioma	Inglés
Compatibilidad	iPhone e iPod Touch



Precio	Gratis
Idioma	Inglés
Compatibilidad	iPhone e iPod Touch



>>> IPHONIZA TU BLOG

Para que cualquier persona que tenga un iPhone pueda navegar por su website favorita existen varios programas que permiten a los blogeros iphonizar sus blogs. Te proponemos alguno de ellos a continuación:

BLOG2IPHONE

Es un programa muy sencillo de utilizar: registrándose en la página http://blog2iphone.com/ agregas la dirección del sitio web y te dan un código. Este código se inserta en la plantilla del blog y en caso de que un usuario entre desde el iPhone, le redirecciona a la versión generada.

INTERSQUASH

Este servicio te permite crear una versión de tu blog para el iPhone al instante, eso sí, la página debe disponer de canal RSS porque es casi lo único que se introduce, la URL del feed de la web junto con el título, y en el siguiente paso, opcionalmente, una imagen. De esta manera, proporciona el código que hay que introducir en el blog para dirigir al usuario del iPhone a la dirección a la página en InterSquash.

ANDANZA

Este servicio adapta tu blog en sólo tres pasos que consisten en, primero indicar la dirección del sitio web, segundo comprobar el resultado y modificarlo al gusto y, finalmente, obtener una dirección del tipo http://m.andanza.com/tublog. Como en el caso anterior la web debe tener un servicio RSS o ATOM y soportar la tecnología OpenSearch.

TYPEPAD

Esta herramienta únicamente permite manejar blogs del servidor del mismo nombre.

Sin embargo, al integrase con TypePad en el escritorio se obtienen todas las características al instante: cuelga de manera rápida y eficiente el post en el blog o lo guarda en forma draft para publicarlo más tarde.

WORDPRESS

Sólo sirve para publicar en este servidor. Permite ver los artículos ya publicados en el blog y editarlos para corregirlos o ampliarlos. Ofrece la posibilidad de incluir más de una fotografía por artículo y crear entradas de texto y guardarlas como drafts para subirlas posteriormente. De esta forma es posible establecer varios artículos en la calle y subirlos cuando lleguemos a casa o a la oficina usando nuestra red Wi-Fi, más rápida y económica.

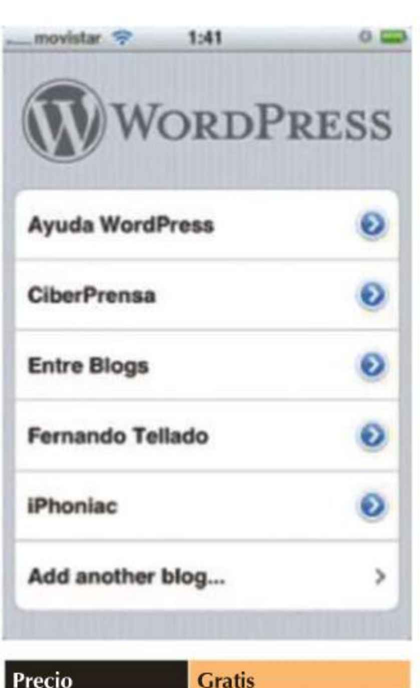
TUMBLE

Para blogs pertenecientes a Tumbar, esta aplicación facilita la creación de post, links, fotos y citas de una manera muy rápida ya que pone a disposición del usuario cinco tipos de post para no tener que hacer esperar a los seguidores de la web.



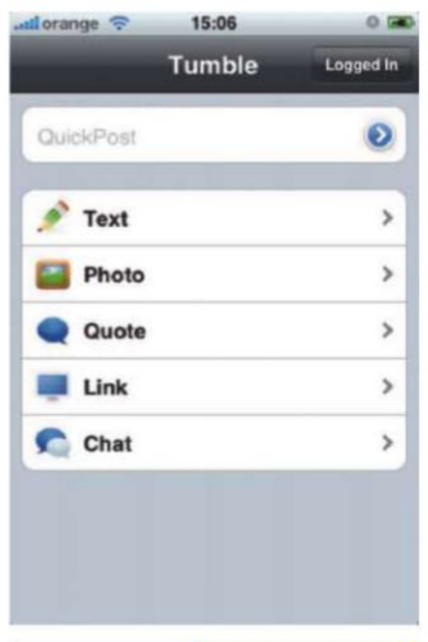


Precio	Gratis
Idioma	Español
Compatibilidad	iPhone e iPod Touch





Precio	Gratis
Idioma	Inglés
Compatibilidad	iPhone y iPod Touch



Precio	Gratis
Idioma	Español
Compatibilidad	iPhone e iPod Touch

OFERTA DE SUSCRIPCIÓN

25%

DE DESCUENTO

12 números a un precio único

44,55 euros

TRUCOS WINDOWS: CONTROLAR A DISTANCIA EL ORDENADOR

@RROBA 144

SEGURIDAD WI-FI
HACK.NET
CREACIÓN DE BLOGS
LA MOVILIDAD

Protege tu móvil y portátil

Y ADEMÁS... CRIPTOGRAFÍA RETROINFORMÁTICA

Más fácil en www.mcediciones.com

Envía este cupón a:



MC Ediciones, S.A.
Passeig de Sant Gervasi, 16-20
08022 Barcelona

Precio ejemplar 4,95 euros
Suscripción España 44,55 euros
Suscripción Europa 103,95 euros
Suscripción resto mundo 163,35 euros.

☐ Deseo suscribirme a @rroba por un año (12 números) al precio especial de 44,55 euros

Según la ley 15/1999 de protección de datos personales, los datos que Vd. nos facilita serán incluídos en el fichero de MC Ediciones, S.A. para la gestión de la relación comercial con Vd. Los datos facilitados son estrictamente necesarios, por lo que su cumplimentación es obligatoria. Asimismo, Vd. consiente expresamente a MC Ediciones, S.A. para recibir comunicaciones comerciales de sus productos y servicios, así como de productos y servicios de terceros que puedan resultar de su interés. Vd. tiene derecho de acceso, rectificación, oposición y cancelación, que podrá ejercitar comunicándolo por carta a: MC Ediciones, S.A. (Paseo San Gervasio, 16-20, 08022 Barcelona).

Nombre y apellidos .... NIF o CIF ....

Dirección .... Teléfono ....

Población .... Provincia .... C.P. ....

Email ....

Para mayor comodidad puede suscribirse a través de nuestra web: www.mcediciones.com / suscripciones@mcediciones.com

FORMA DE PAGO

☐ Adjunto talón bancario

☐ Tarjeta de crédito

☐ VISA (16 dígitos) ☐ American Express (15 dígitos)

Tarjeta nº

Caducidad

Titular tarjeta o cta. cte.

Firma

☐ Domiciliación bancaria (Datos Banco/Caja)
Con renovación automática hasta su orden.

Banco o caja

Entidad oficina d.c. nº de cuenta



144

AÑO 9 (??? ¿YA?), NÚMERO 144

FRIKI GADGET
LO MÁGICO DE UN DíA DE COMPRAS

De tu puño y letra, en el PC

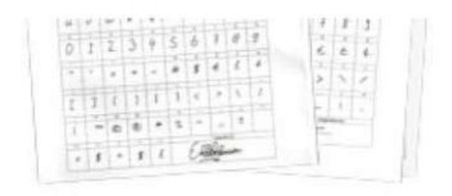
El hazlo tú mismo (do-it-yourself; DIY) es una filosofía muy amplia que abarca desde una casa hasta una bufanda, pasando por las consabidas chapuzas domésticas e informáticas. En esta ocasión se trata de un DIY no exento de glamour y de originalidad. Desterrar la Times New Roman o la Arial de nuestros documentos de texto y substituir estas tipografía por una ya no solo creada por uno mismo sino basada en nuestra letra manuscrita es algo muy exclusivo y geek. De esta manera le daremos un toque personal a nuestros textos e incluso podremos obtener, mediante esta aplicación, un inusual regalo. En **http://www.yourfonts.com** encontramos un generador de fuentes online, que nos permite crear en unos 15 minutos nuestra propia tipografía OpenType, de más de 200 caracteres, a partir de nuestra letra manuscrita. También se incluye la digitalización de la firma, por si la queremos usar para firmar documentos digitales.

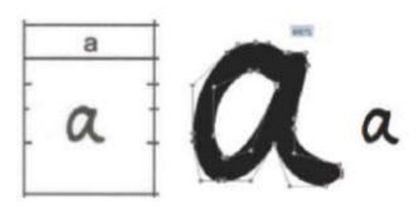
Aunque se trata de un servicio con coste – puede rondar unos 10-15 dólares, según las taridas que se mencionan en la web- es posible previsualizar el resultado antes de efectuar el pago. Por lo tanto, solo compraremos si quedamos satisfechos con el resultado. Las tipografías creadas se pueden usar en cualquier sistema operativo: Windows, Mac OS X o Linux.

Despacito y buena letra y ¡a esmerarse con la plantilla!

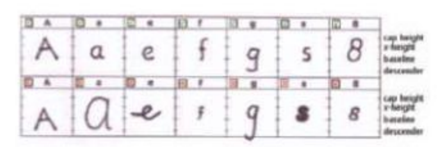
Para empezar a usarlo solo hay que descargar e imprimir una plantilla que hay que rellenar de nuestro puño y letra. Aunque la web sólo está en inglés, el servicio permite crear tipografías para otros idiomas como francés, alemán y español, entre otros. De hecho ha sido muy gratificante comprobar que, entre los 200 caracteres, han incluido nuestra querida e indispensable eñe. Una vez se ha cumplimentado la plantilla, ésta se escanea y el archivo resultante (JPG, TIF, PNG, etc) se guarda y posteriormente se carga en la aplicación. En tan solo 15 minutos podremos previsualizar el resultado. Y si nos convence, entonces comprarlo, descargarlo y empezar a usarlo. Y a juzgar por los numerosos comentarios dejados por los usuarios del servicio, suele ser así en la mayoría de los casos. Hay que destacar también que los de Yourfonts.com se han tomado la molestia de explicar también cómo se ha de instalar una fuente en cada sistema operativo para que ésta funcione. Aunque si se trata de un regalo, este último paso debería estar incluido en el pack, ¿no?

Por cierto, si se os ocurre que es una genial idea y habéis pensado en ello como regalo de Navidad, haced números pues la empresa High-Logic también comercializa paquetes de software para generar tipografías. FontCreator, el más popular y con una versión de prueba para descargar, cuesta unos 79 dólares en su versión para uso doméstico. <





ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
01234567890!@#$%&*(){}[]<>?
Creating my own font was fun,
and using it is even better!



Y ahora, a cambiar la música





Y una más de personalizaciones, en este caso del teléfono móvil. Hace tiempo que se dice que este dispositivo omnipresente se ha convertido en una extensión de nosotros mismos y por tanto queremos que refleje nuestra personalidad. La creación de melodías o ringtones es un nivel más. Si estás cansando de llevar el mismo tono que la mayoría de los mortales y te ha venido la vena artística, ésta es tu oportunidad. Una vez más puede ser un original e inesperado detalle que podemos enviar a su destinatario por correo electrónico.

En **http://makeownringtone.com** se pone a disposición del interesado un programa online gratuito para poder crear tonos de llamada con la música que más nos guste y los efectos que queramos añadir. Para adecuarse a todos los niveles de usuario, el generador cuenta tres opciones: básico, avanzado y experto, ampliándose sustancialmente las funcionalidades de una a otra opción.

La aplicación está disponible online, es decir, no necesita ser descargada. Por ello una vez estemos en la página web mencionada anteriormente, lo primero que hay que hacer, sea cual sea el nivel que vayamos a elegir, es subir un archivo de audio, ubicado en el ordenador. El programa permite trabajar con diferentes formatos - MP3, MP4, OGG, ACC, entre otros. Una vez el archivo está cargado en la aplicación se puede seleccionar el fragmento sobre el que trabajar. Aunque también se puede hacer sobre la totalidad del archivo. Como la modalidad básica es bastante limitada (solo nos permite normalizar -audio sin distorsiones -y crear fundidos) directamente es recomendable entrar a valorar la avanzada o la experta. En esta última cuenta con 18 opciones entre las que destacan -por llamativas- las que permiten crear eco, reverberaciones o crear efecto de coros. También es posible modificar aspectos como la frecuencia de los agudos o de los bajos, o la velocidad. Así se puede cambiar la calidad de sonido que tiene por defecto o aplicar filtros para dar diferentes efectos a la melodía.

Una vez se ha trasteado con el archivo de audio, aplicando un efecto y otro, probando, deshaciendo y volviendo a probar, y estamos complacidos con el resultado – suerte que existe la opción 'deshacer'- solo queda convertir el archivo a un tono de llamada. El programa nos ofrece tres vías para descargar el archivo creado con nuestra intervención artística: en el mismo ordenador, enviándolo a una dirección de correo electrónico o enviándolo al teléfono móvil directamente, que sería lo suyo, pues es allí donde va a sonar. <

Ecos, coros, reverberaciones,... cualquier efecto puede servir para tu propio ringtone

Tus fotos en un portátil de pared

Seguro que se nos ocurren muchas cosas para hacer con un portátil viejo. Una que pasa por seguir aprovechando su vida útil al máximo, sin que su escaso rendimiento nos afecte ya, consiste en convertirlo en un marco de fotos digital de pared. ¿Todo ello siguiendo una ingeniosa idea de Justin Grisworld, detallada en su blog GlowView: **http://blog.glowview.com/2009/03/20/custom-self-contained-hanging-wall-pc/**

Convertir un viejo ordenador portátil en un marco digital de pared ofrece ventajas tales como una ocupación mínima de espacio y la posibilidad de ampliar la pantalla del ordenador de mesa, entre otras cosas. Además, y lo más importante, es que no supone un gasto extra ya que no se compra un marco sino que se aprovecha un portátil casi en desuso. Y como se trata de este dispositivo, sus funcionalidades van más allá de las de un marco estándar siendo posible ver películas, la televisión y escuchar música. En el caso de que sea wireless, además podremos seguir usándolo para navegar por Internet o ver videos de Youtube.



Según las indicaciones de Justin Grisworld, el desmantelamiento del portátil es relativamente fácil y solo es cuestión de ir quitando los diminutos tornillos para extraer cada pieza en el orden correcto y separar el marco del respaldo de la pantalla. Si te puedes hacer con el manual de montaje de tu portátil lo tendrás más fácil. Una recomendación que realizar el promotor de esta iniciativa es tener mucho cuidado ya que los ordenadores portátiles suelen tener las antenas de inalámbricas colocadas en el interior de la tapa superior de cada lado de la pantalla LCD. Interesa preservarlas, además de la conexión inalámbrica, para su uso. Evidentemente este proceso puede variar entre los diferentes modelos de portátiles.

La pantalla se anexa por la parte de atrás a la parte inferior del portátil, cruzando los dedos para que todo cuadre, y se ata para que se mantengan unidos, usando cinta de doble cara, como comenta el autor del blog. Al parecer, lo más complicado de todo el proceso, es encontrar un marco que haga las veces de frontal.

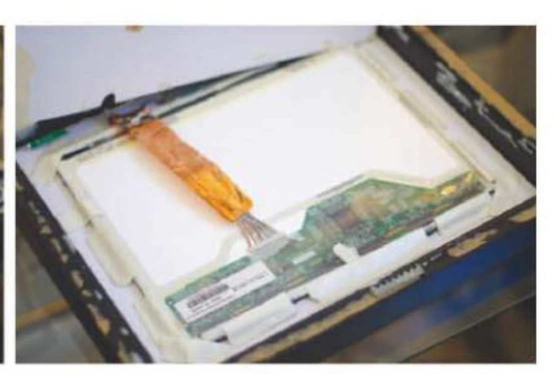
Para controlar las funciones del nuevo marco digital se puede usar un ratón inalámbrico o hacerlo de manera remota (remote desktop, VNC, etc). Otro detalle a tener en cuenta es el peso del portátil, que en el caso del ejemplo, era de unos 2 kilos. También es importante que quede espacio entre el marco y la pared para que el dispositivo pueda ventilar correctamente. <



No tires tu viejo portátil: dale un uso decorativo, colgándolo de la pared







Paquito y Flecha, ¡vaya par!

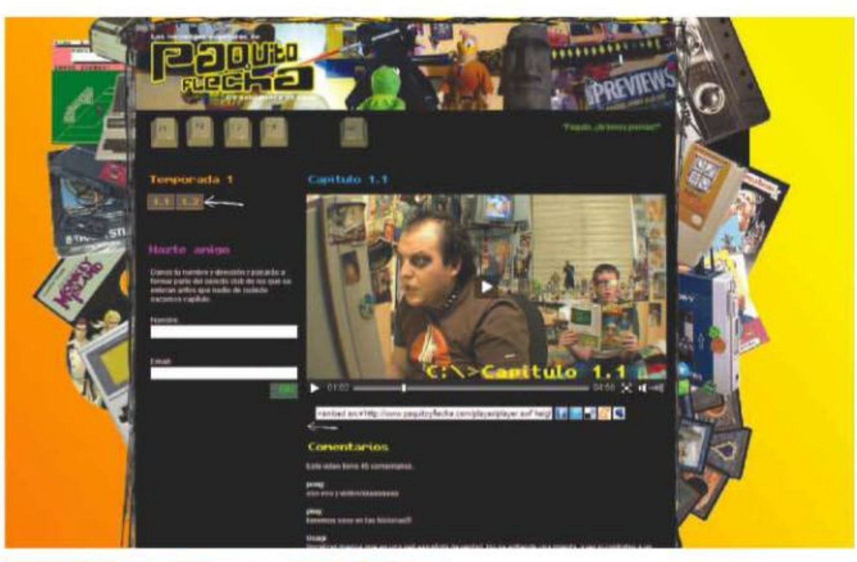
Esta semana hemos recibido en la redacción un correo electrónico algo inquietante. El remitente es alguien que no conocemos y que se presenta como la vecina de Paquito, quien le ha encargado el marketing y RR.PP. de la serie han lanzado en Internet: Paquito y Flecha. La serie cuenta las aventuras y desventuras de Paquito, un hikikomori (esos japoneses que no salen de su cuarto ni a tiros) de Móstoles, y su fiel escudero Flecha, un tipo un poco raro de pasado oscuro que le acompaña y le hace de vínculo con el mundo exterior. Todo esto en capítulos de unos cinco minutos que transcurren en el cuarto de Paquito como único escenario. ¿Conseguirán un hilo narrativo coherente con estas restricciones? Eso está por ver. Por el momento tienen dos capítulos en su web **http:// www.paquitoyflecha.com**, que ya sirven para hacerse una idea de por dónde van los tiros e ir conociendo a los dos personajes principales. Según comenta uno de sus autores, Paco Ponce de León, en su blog **http://www.pudeseralguien.com**, Paquito y Flecha es una serie nacida de los desvaríos mentales de Eduardo Iglesias, Naiel Ibarrola y un servidor. Es una serie de ficción que en ocasiones se salta la cuarta pared y juega con el meta-lenguaje. Y está basada en nuestras vidas un poquito más de lo que nos gusta aceptar. Es un producto indie a más no poder, dónde todos desempeñamos numerosos roles, siendo yo mismo co-guionista, director de fotografía y actor".

Como podréis comprobar nada más verla, la serie se está rodando con todos los adelantos tecnológicos, "robados directamente a James Cameron en una excursión que se hizo el Flecha a Disneyworld", nos ha cotilleado la vecina. Aunque el plató no está ubicado en La Ciudad de la Luz precisamente.... Otro cotilleo que nos ha llegado a través de la vecina chismosa es que, al parecer, habrá cameos de actores famosos e incluso algún capítulo dirigido por directores invitados de calado nacional. ¡A ver a quién consiguen engatusar para que se apunte! De momento se curan en salud y no sueltan ningún nombre no sea que al final no salga y queden fatal. Para animar al personal anuncian que dentro de poco también habrá concursos y secciones donde se podrá participar y ganar 'apetecibles' premios como chapas con los caretos de Paquito y Flecha o cenas románticas con alguno de ellos. No sé quién participaría en un concurso para irse a cenar con estos dos pero siempre hay un roto para un descosido...Por lo pronto, en cuanto a temas de participación, podemos dejar plasmados nuestros comentarios y opiniones tras ver los dos primeros episodios colgados por el momento.

Para amenizar la espera del tercer capítulo, ambos elementos tienen un blog - (No sin mi wifi) **http://www.paquitoyflecha.com/blog** - que actualizan diariamente ellos mismos, o eso dicen. De momento tienen algunos posts curiosos sobre sus cosas y su gente, como éste en el que publican las fotos de algunos amigos de Paquito:

http://www.paquitoyflecha.com/blog/2009/07/27/los-amigos-de-paquito-50-fotos-de-nerds/

Y es que, a pesar de no salir nunca de su cuarto, Paquito tiene una intensa vida social cuya banda sonora es el ruido del teclado y las campanitas del messenger. <



Llegan a Internet las aventuras y desventuras de Paquito y Flecha, dos frikis de cuidado







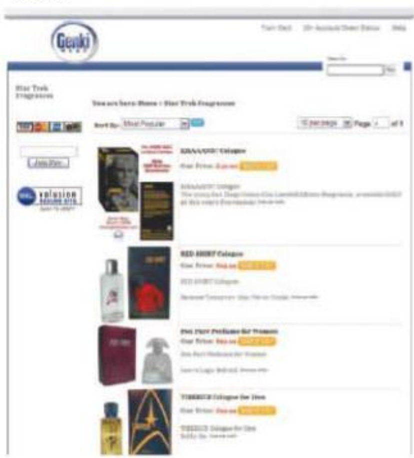
Oler como una estrella





Y más concretamente, como una de Star Trek. Por si nos cabía alguna duda, el mundo trekkie es de los más frikis de todos los tiempos. Y es que, leemos en PopGadget **http://www.popgadget.net/2009/07/smell_like_star.php#more** que el fabricante de perfumes Genki Wear ha lanzado en la presente edición de la Comic Con de San Diego una nueva fragancia que se añade a la familia ya existente: la KHAAANN! COLOGNE. Se trata de la primera San Diego Comic-Con Limited Edition Fragrance, de la que han puesto a la venta solo 500 frascos para ser vendidos en todo el mundo.

El aroma está inspirado en el personaje de Khan Noonien Singh, un ficticio dictador del siglo XX, interpretado en la serie original y en la película Star Trek II: La ira de Khan por el actor Ricardo Montalbán. De naturaleza alterada genéticamente, este hombre poseía una fuerza e inteligencia por encima del promedio y llegó a dominar una cuarta parte del planeta Tierra.



Pero la perfumera Genki Wear, que se ha hecho un nombre en los anales de la cultura geek-pop con sus perfumes y colonias inspirados en StarTrek, tiene otras disponibles en su catálogo. RED SHIRT Cologne se orienta los hombres jóvenes y modernos de la Galaxia, que no vacilan, que se muestran vivos. Según sus creadores, esta fragancia instila confianza, mostrándole al universo la fuerza, el valor y la devoción de quien la usa por vivir cada día como si fuera el último. "Porque el mañana quizás nunca llegue", reza su eslogan. En cuanto al aroma, la definen como brillante, limpia y directa con notas de mandarina verde, bergamota y lavanda en la superficie pero con una base de cuero y de almizcle gris.

También han pensado en las trekkies féminas o en las abnegadas novias/esposas de los trekkies más consumados y por ello cuentan en su catálogo con Pon Farr Perfume. "Deja la lógica atrás" es el eslogan, "porque tener algo no siempre es tan placentero como desearlo". Y es



Toda una gama de perfumes trekkies de la mano de Genki Wear

que el Pon Farr engloba, en la sociedad vulcana, los síntomas que avisan de que ha llegado la etapa de apareamiento que tiene lugar cada siete años. Genki Wear dirige este perfume a mujeres que quieren una fragancia refrescante que sea vigorizante a la vez que delicada, con ligeras notas superiores de fruta cítrica, grosella negra, flor de loto y lirio de agua y con una base de sándalo, melocotón y mora.

La última de la familia de perfumes trekkies es TIBERIUS Cologne, inspirada en el famoso James Tiberius Kirk, capitán de la nave estelar Enterprise NCC-1701 y NCC-1701-A. Esta colonia para hombres incorpora los ingredientes del valor y el espíritu, aunando la química y la emoción. Según describen sus creadores, TIBERIUS es una fragancia ocasional aderezada con notas de frescura y sensualidad. Ingredientes como el cítrico dulce, la pimienta negra y el cedro contribuyen a crear una fragancia refrescante con una base de cálida vainilla, almizcle blanco y sándalo. "Difícil definir, imposible rechazar. En cualquier universo", aseguran los de Genki Wear.

Las cuatro colonias, en botellas de 100 ml, se venden a todo en mundo **http://shop.genkiwear.com/Star_Trek_Fragrances_s/91.htm**

y sus precios oscilan entre los 29,99 y los 40 dólares, gastos de envío aparte. <

Cool-geek Sneaker

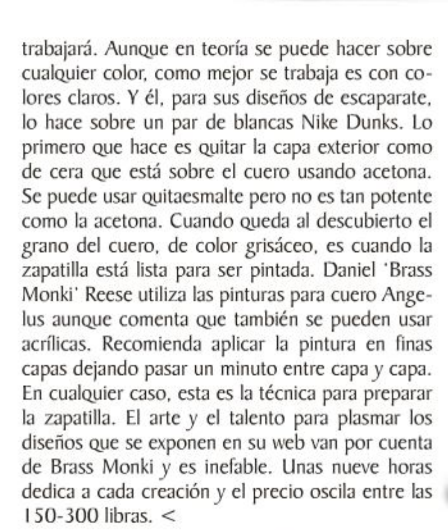






Gracias al blog de Paquito y Flecha nos hemos enterado de esta página web donde se ofrecen unos extraordinarios diseños para personalizar tus zapatillas de deporte. Si eres un 'sneaker freaker' no te puedes perder la web de Daniel Reese AKA Brass Monki **http://brassmonki.wordpress.com**.

Como se muestra en las imágenes Brass Monki personaliza zapatillas deportivas, desde las suelas hasta las cordoneras, con temáticas de lo más variadas que van desde las películas como Kill Bill, Robocop hasta los videojuegos -Final Fantasy, Super Mario Bros, Zelda o Tetris - pasando por cómics como Hulk, Capitán América, Sin City o IronMan y personajes reales y de ficción como los Beatles, Pikachu, Sonic, Minnie Mouse, C3P0 y R2D2.



Vaya, que hay mucho dónde elegir. A destacar el éxito desmedido que están teniendo entre los fans del Michael Jackson las personalizaciones con diseños homenaje al difunto Rey del Pop: Thriller, Jackson, Off The Wall, Tribute y GOLD or Bad.

Aunque los diseños mostrados en la página web son solamente conceptos, basta con elegir uno para que, gracias a la técnica y al talento de Reese se conviertan en realidad.

Y es que Brass Monki trabaja por encargo, elaborando cuidadosamente el diseño elegido por el usuario de entre el amplio catálogo que muestra en la web. Pero también se le pueden hacer propuestas. Así, por ejemplo, si tienes la espinita clavada con algún personaje de los que nunca hay merchadising ésta es una buena forma de resarcirse. Este es el caso de AJ Glasser que en http://kotaku.com/5315627/at-long-last-moogle-shoes-sort-of cuenta lo mucho que cuesta encontrar artículos fashion de Moogle de Final Fantasy y que justamente Reese sí que tiene un diseño con ese personaje.

Sabedor de que la técnica no es todo, Brass Monki no duda en explicar cuál es el proceso que emplea para preparar las zapatillas deportivas sobre las que trabajará. Aunque en teoría se puede hacer sobre cualquier color, como mejor se trabaja es con colores claros. Y él, para sus diseños de escaparate, lo hace sobre un par de blancas Nike Dunks. Lo primero que hace es quitar la capa exterior como de cera que está sobre el cuero usando acetona. Se puede usar quitaesmalte pero no es tan potente como la acetona. Cuando queda al descubierto el grano del cuero, de color grisáceo, es cuando la zapatilla está lista para ser pintada. Daniel 'Brass Monki' Reese utiliza las pinturas para cuero Angelus aunque comenta que también se pueden usar acrílicas. Recomienda aplicar la pintura en finas capas dejando pasar un minuto entre capa y capa. En cualquier caso, esta es la técnica para preparar la zapatilla. El arte y el talento para plasmar los diseños que se exponen en su web van por cuenta de Brass Monki y es inefable. Unas nueve horas dedica a cada creación y el precio oscila entre las 150-300 libras. <

Tetris, Robocop, Michael Jackson... ¿qué diseño elegirías?











FRIKI GADGET



Gladiator 600, gran capacidad de refrigeración

Proporcionar el mejor flujo de aire es el objetivo de este producto que ofrece la posibilidad de instalar en su interior hasta cinco ventiladores de 120 mm. La nueva caja Gladiador 600 de CoolerMaster, distribuida por Sistemas Ibertrónica, es un chasis robusto con increíble capacidad de refrigeración. Con formato de media torre, compacto y resistente, el Gladiator 600 tiene un frontal dotado de un ventilador con LED azul que se puede controlar directamente a través del regulador colocado en dicho frontal. Además cuenta con un sistema de ventilación en los paneles superiores y laterales y su ventilador de 140mm situado en la parte superior. Permite colocar la fuente de alimentación en la parte inferior de la caja y facilita la instalación de los componentes en su interior, gracias a algunos slots destinados a montaje y al no requerir el uso de herramientas para dicha tarea. A toda esa lista de prestaciones se añade una excelente gestión de los cables para garantizar buenas conexiones, favoreciendo la refrigeración interna y evitando el posible daño de alguno de los componentes. **www.ibertronica.es**

imax mini, ordenador de sobremesa de bajo coste

Para aquellos que buscan un dispositivo que pueda realizar las mismas tareas que un ordenador de sobremesa en un tamaño extra pequeño, Packard Bell ofrece imax mini, un sobremesa de bajo coste diseñado para navegar en Internet, comunicarse en las redes sociales, disfrutar del contenido digital y, ocasionalmente, para juegos. Ultrafino y ultrapequeño, se puede conectar en la parte trasera de cualquier monitor o ubicarse en una mesa en su soporte de pie y conectarse directamente al televisor sin ningún problema. Incluye un mando giroscópico que se puede utilizar como control de videojuegos o como mando a distancia multimedia inteligente gracias a su ratón que funciona en el aire. El imax mini de Packard Bell está equipado con un procesador Intel Atom y un chipset NVIDIA ION; además integra 2 GB de memoria, un disco duro de hasta 160 GB, un conector HDMI, lector de tarjetas 4 en 1 y 4 puertos USB. Como opciones de conectividad se incluyen puertos Wi-Fi y LAN. Se suministra de serie con un mini teclado, un ratón óptico y un control de videojuegos. El conjunto de juegos de imax mini incluye el juego de acción SEGA Sonic Heroes, SEGA Sonic Riders y el de carreras SEGA Crazy Taxi 3. Disponible en dos versiones, Microsoft Windows XP Home Edition o Microsoft Windows Vista preinstalado, el ordenador tendrá un precio estimado de 199 euros y 249 euros respectivamente. **www.packardbell.es**

Fotos a prueba de clima

De la mano de Grup Strand 87 llega Dry Pack de Allsop, una funda protectora para pequeños dispositivos digitales con la que las condiciones atmosféricas dejarán de ser un impedimento a la hora de hacer fotografías - con lluvia, nieve e incluso bajo el agua - o escuchar tus MP3 favoritos. Esta práctica funda, con unas medidas de 200 x 120mm, garantiza el cierre hermético y la absoluta protección del material que alberga: una cámara fotográfica digital, un MP3 o cualquier dispositivo electrónico. Además con ella se evita el deterioro causado por la acción de la humedad, el viento, el polvo u otras agresiones externas. La Dry Pack está fabricada en poliuretano transparente, con triple sellado de seguridad para una resistencia total frente al agua, incluso en inmersiones de hasta tres metros de profundidad. Esta funda polivalente dispone de una ventana para hacer fotografías sin renunciar a la mejor calidad de imagen y se presenta con una práctica correa ajustable. **www.grupstrand.com**





Cometas 3D Star Wars

Ya están aquí. Acaban de aterrizar en España las míticas naves espaciales de la Guerra de las Galaxias: Halcón Milenario, Caza Rebelde X-Wing y Caza Imperial Tie Fighter. Las nuevas cometas de Star Wars, con casi un metro de largo y en formato 3D, serán la sensación de este verano. Aunque éstas no vuelan por el espacio, su impresionante diseño en 3D de un metro de longitud dejará boquiabiertos a todos aquellos que se crucen en su camino. Las cometas Star Wars son un fiel reflejo de las naves en 3D. De fácil montaje, miden casi un metro de longitud y no son planas, sino que están hechas en 3D para dar más realismo a la nave. Además, al estar fabricadas en nylon ripstop son capaces de aguantar fuertes ráfagas de viento. Su estructura es muy resistente, no sólo gracias a su tejido en nylon, sino también a su estructura de varillas de fibra de vidrio. Los fans de la mítica saga de las Guerra de las Galaxia están de suerte y podrán adquirirlas en **www.planetapluton.com**

Las videocámaras son para el verano

¿Eres de playa o de montaña?, ¿eres de los que preparan equipaje maxi o de los que ni facturan en el aeropuerto? Seas cómo seas, MEDION te pone fácil disfrutar de una videocámara, optando por la que más se ajusta a tus necesidades. Si te encanta pasar el día remojo, ahora tienes la nueva videocámara MD86066 Underwater, que dispone de una carcasa especial que la convierten en sumergible, que le permite de resistir bajo el agua hasta una profundidad de 5 metros. Cuenta con una resolución de 5 megapíxeles, lector de tarjetas de memoria SD/SDHC, salida HDMI e interface USB 2.0 y dispone de una pantalla de visualización de 6 cm. En cambio si disfrutas perdiéndote entre las montañas, la cámara MD86064 Sports está hecha para ti: cuenta con 90 MB de memoria interna para grabar tus expediciones, es resistente a salpicaduras de agua y dispone de grabador de voz, de vídeo y reproductor de música en un único dispositivo. Además admite tarjetas de memoria SD y SDHC y tiene unas medidas que hacen que pueda confundirse con un simple teléfono móvil: 6,4x10,5x2,2 cm. Y si los equipajes pequeños y compactos son lo tuyo, no te pierdas la cámara MD 85961 HD ultradelgada que, con sólo 2 cm de grosor, cabe en cualquier parte. Dispone de 34 MB de memoria interna y pantalla de visualización rotatoria de 2,5 pulgadas. También incluye reproductor MP3 e incorpora salida HDMI, admite tarjetas de memoria SD y SDHC, dispone de mini puerto USB 2.0. **www.medion.com**





Chasis Xenic 6030, el de Transformers

Maxcube hace un guiño a los seguidores de la mítica serie Transformers con el chasis Xenic 6030, una caja tipo torre confeccionada en aluminio de gran resistencia, con unas dimensiones de 200 x 475 x 515 mm (incluyendo bisel) y confeccionada para ser compatible con placa base ATX y Micro ATX. Fabricada íntegramente en aluminio de color negro y con acabados en gris metalizado, esta caja se presenta como solución perfecta para todos los gamers y entusiastas del PC. Una apuesta futurista que destaca por su eficiente sistema de refrigeración, ya que viene equipado con dos potentes ventiladores: uno frontal de 12cm con iluminación LED azul y uno trasero de idénticas características. Así, la incorporación de estos ventiladores unida a su bisel lateral de malla metálica asegura un constante flujo de aire para refrigerar de forma eficaz todos los componentes del equipo. El Xenic 6030 es compatible con fuentes alimentación ATX PS2 o EPS. Se presenta con las mejores opciones de expansión gracias a sus cuatro bahías externas para albergar unidades de 5,25", dos para 3,5" y otras cuatro internas para unidades de 3,5". Además, para una máxima ampliación del sistema, está provisto de 7 slots de expansión, cuatro puertos USB 2.0 y uno eSATA, así como una entrada de audio HD y otra de micro. **www.maxcube.com**

FRIKI GADGET







Manos libres en tu viaje por carretera

Tanto si viajas en coche como en moto, Parrot te propone dos de sus últimas soluciones para que tu experiencia al volante – o al manillar- sea más cómoda, segura y placentera: su gama para el automóvil Parrot MKi y el kit para motos Parrot SK4000. Los nuevos manos libres Parrot Mki, diseñados bajo licencia oficial de Apple, te permiten viajar tranquilo y disfrutar de toda tu música mientras vas al volante. Puedes conectar tu iPod, iPhone o tu MP3 o memoria USB al manos libres y escuchar tu lista de canciones directamente en los altavoces del coche. También puedes conectarle cualquier dispositivo Bluetooth Estéreo (A2DP): MP3, teléfonos móviles, smartphones… Al igual que los demás kits de Parrot, la gama MKi es compatible con Bluetooth e incorpora los últimos avances en sistemas manos libres para el coche: sincronización automática de la agenda de contactos, reconocimiento de voz multiusuario, síntesis vocal de los nombres de la agenda, gestión de contactos (hasta 2.000 por teléfono), identificación vocal del interlocutor, etc…Por otro lado el Parrot SK4000 es un completo kit manos libres Bluetooth diseñado especialmente para motos. Incluye un sintonizador FM/RDS, una entrada de línea y también conectividad Bluetooth Estéreo (A2DP). El dispositivo sincroniza y actualiza automáticamente la agenda con los contactos del teléfono móvil e incorpora reconocimiento de voz multiusuario. Está especialmente diseñado para eliminar el ruido exterior, lo que proporciona más calidad y claridad de sonido en un entorno altamente ruidoso.

www.parrot.com/es

¡A bucear se ha dicho!

…con Camera Mask Pro, estas gafas profesionales de bucear que incorporan una cámara de 5 megapíxeles para hacer fotos y grabar videos con sonido bajo el agua. Con ellas no sólo se puede bucear por la superficie, sino también sumergirse hasta 10 metros de profundidad para fotografiar el fondo marino. Además, viene con una memoria interna de 16 MB con posibilidad de ampliar la capacidad al insertar una tarjeta de memoria Micro SDHC de hasta 8 GB. De esta manera, cuentan con la capacidad suficiente para realizar fotos durante todo el verano sin necesidad de descargarlas. Para usarla, una vez estés sumergido, tan sólo tendrás que pulsar el botón que se encuentra en la parte superior derecha. El paquete viene con unas gafas de bucear con cámara acuática integrada, manual de usuario, cable USB y software ArcSoft para edición de fotos y vídeos. El precio de venta son 139 euros.


www.planetapluton.com





Auriculares deportivos de colores

Los auriculares Panasonic se han diseñado para dar respuesta a la necesidad de escuchar música con calidad mientras se realizan deportes con una intensa actividad. Por eso se han impermeabilizado al agua y al sudor y se les ha dotado de una forma ergonómica. Gracias a su gancho de elastómero totalmente flexible que se sujeta cómodamente a la oreja, los auriculares se adaptan a la perfección a los movimientos del deportista. Su cable de 1,2 metros no entorpece los movimientos y su reducido peso, 14 gramos, es todo un alivio. El RP-HS33 de Panasonic ofrece una frecuencia de respuesta de 14Hz-24Hz y se comercializa en color azul turquesa, rojo, negro, naranja y verde. Estos vivos colores se corresponden a la perfección con los mismos colores de iPod nano. El PVPR (IVA incluido) del RP-HS33 es de 15,99 euros. **www.panasonic.es**

Más almacenamiento y velocidad para los netbooks

Disponible en capacidades de 8 y 16GB, la tarjeta SDHC para netbooks de SanDisk permite a los usuarios ampliar el almacenamiento manteniendo al mismo tiempo las ventajas de tamaño y coste. Al insertar la tarjeta en una ranura para tarjetas de su ultraportátil, se añade capacidad de forma instantánea. Puesto que la tarjeta reside dentro del ultraportátil, se reduce el riesgo de que se dañe mientras se traslada el equipo. Asimismo, la compañía ha comenzado a distribuir sus unidades de estado sólido (SSD) de nueva generación basadas en memoria flash para ultraportátiles, que incorporan componentes de alto rendimiento a un precio competitivo. Las unidades pSSD P2 y S2 de SanDisk emplean nCache, una tecnología de escritura no volátil que aumenta hasta cinco veces el rendimiento de la escritura aleatoria frente al rendimiento en estado fijo. Las pSSD P2 y S2 ofrecen 9.000 vRPM de rendimiento en estado estático además de nCache, que va más allá y ofrece una caché no volátil de hasta 320MB para soportar ráfagas de instrucciones de escritura aleatoria que maximizan la respuesta del sistema. Además, y dado que nCache es no volátil, los datos del usuario están siempre protegidos. **www.sandisk.com**





Trabaja en equipo con MIFI

Vodafone España amplía su gama de dispositivos de Internet Móvil para trabajar en equipo con el lanzamiento del dispositivo móvil wifi "MiFi", disponible para clientes de empresa y particulares. Diseñado por Novatel Wireless, el nuevo "MiFi" integra tecnología HSPA (High Speed Packet Access) y permite que hasta 5 dispositivos wifi (portátiles, pda, videoconsolas, etc) se conecten a Internet de forma simultánea con sólo darle a un botón, compartiendo entre ellos una conexión de Internet Móvil. Además incorpora una batería interna con hasta 4 horas de autonomía y tiene un tamaño ligeramente superior al de una tarjeta de crédito. Está disponible desde 29 euros para los clientes de empresa y particulares. En ambos casos, está ligado a la contratación de una tarifa de datos de Internet Móvil. **www.vodafone.es**

FRIKI GADGET



Súper zoom híbrida con 18x y grabación de vídeo en Alta Definición

Panasonic presenta una nueva Lumix híbrida, la DMC-FZ38, que combina la grabación de vídeo en formato AVCHD Lite, que permite grabar el doble de imágenes en alta definición, y la captura de imágenes en alta calidad con un potente gran angular de 27mm y un súper zoom óptico de 18x LEICA DC VARIO-ELMARIT con luminosidad F2.8. Además, la FZ38 también incorpora el modo Intelligent Auto de Panasonic para la grabación de imágenes en movimiento. Incluye, además, POWER O.I.S., un estabilizador óptico de imagen que dobla la capacidad de reducción de los temblores al sujetar la cámara en comparación con el sistema de estabilización de imagen convencional MEGA O.I.S. Al integrar la grabación en AVCHD Lite, se pueden seleccionar tres niveles de calidad para las imágenes en movimiento: SH (17 Mbps), H (13 Mbps) y L (9 Mbps). La FZ38 también incluye Dolby Digital Stereo Creator para grabar audio en alta calidad estéreo. El sistema AF de velocidad ultra rápida desarrollado por Panasonic, captura imágenes rápidamente con un tiempo de puesta en marcha realmente ajustado. El modo Ráfaga del sistema multitarea de procesamiento de imagen puede realizar aproximadamente 2,3 disparos por segundo a una resolución de 12,1 megapíxeles. El modo Ráfaga Alta Velocidad consigue aproximadamente unos 10 disparos por segundo y el modo Ráfaga Flash permite tomar disparos consecutivos con emisiones continuas de flash. La DMC-FZ38 de Panasonic tiene un eficiente procesador de imagen que permite realizar hasta 470 disparos con una misma carga de batería. **www.panasonic.es**



Altavoces para PC de alta calidad

Expressionist PLUS (FX3021), de Altec Lansing, combina rendimiento y diseño compacto a un precio atractivo. Este nuevo sistema compacto de atrevido diseño proporciona un sonido natural mediante unos altavoces 2.1 que incorporan un subwoofer cónico integrado en la base. Este subwoofer emplea un driver de 5,25 pulgadas de largo alcance para graves que se extiende hasta 50 Hz, incluso cuando está colocado sobre un escritorio. El control de los graves está al alcance de la mano, lo que permite al usuario conseguir un equilibrio óptimo entre el subwoofer y los satélites duales full range de 2 pulgadas, que completan el sistema. El Expressionist PLUS ofrece una impresionante potencia de 33 vatios y, gracias al diseño Audio Alignment de Altec Lansing, permite alinear los drivers, los periféricos y la electrónica con total precisión para gozar de un sonido natural. El sistema de altavoces para PC Expressionist PLUS FX3021 tiene un precio recomendado de 99,99 euros. **www.alteclansing.com**

¿El final de Dexter, cerca?

Aún en vilo tras los acontecimientos de la tercera temporada de Dexter y mientas estamos contando los días que quedan para el estreno en Estados Unidos, de la mano de Showtime, de la cuarta temporada de la serie del asesino en serie más popular y brillante nos llegan unas noticias de que el final podría estar cerca. Sabemos que nada es eterno, que ninguna serie dura para siempre pero ¿por qué no unas cuantas temporadas más? Y es que, según deja entrever Michael C. Hall en una entrevista en vídeo realizada por Michael Ausiello (y colgada en http://ausiellofiles.ew.com) en el marco de las novedades derivadas de la Comic-Con de San Diego. Así pues esa anhelada temporada -que se estrenará en Estados Unidos en otoño de este año- podría ser la antesala del final de la serie. Y de esta manera la quinta temporada prevista por Showtime podría ser la última las andanzas del 'Oscuro Pasajero' que se ha granjeado las simpatías de millones de espectadores en todo el mundo. Lo vimos salir de su ensimismamiento y su mundo y sociabilizar e iniciarse en los placeres mundanos, compartiendo su secreto e incluso ejerciendo de maestro. En la cuarta temporada el asesino más pulcro y metódico será, además, marido y padre. Es de prever que los guionistas estén desde hace tiempo devanándose los sesos para encontrar el final que nos merecemos los espectadores. <



Get Latest Headlines

Killer 'Dexter' scoop: Is the end near?

Jul 27, 2009, 05:07 PM | by Michael Ausiello
Categories: Comic-Con, Dexter, News

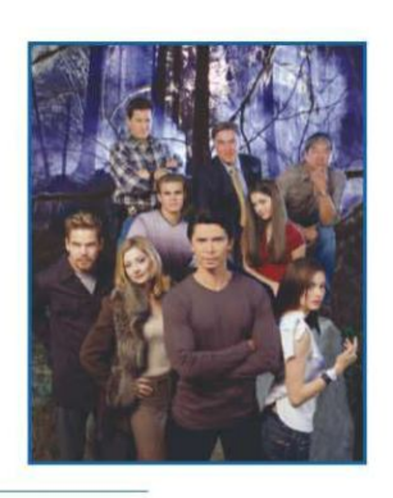
I know you probably don't want to hear this, but *Dexter* is eventually going to die. "It can't last forever," concedes leading man Michael C. Hall. "The show is like a shark. It has to keep moving forward. And if it runs out of things to eat it's going to die." Until then, you get to enjoy exclusive video interviews like the one below. Shortly after receiving a superhero's welcome at Comic-Con, Hall dropped by EW.com's suite at the Hard Rock to chat about season 4, the upcoming *Dexter* prequel, and Showtime's "creepy" ad campaign. Watch the complete interview after the jump. And to see more of my Comic-Con videos, and other interviews and panels, head over to our Con hub.

EW Video





¡Ya queda menos!



Protagonizada entre otros por Robert Carlyle, Stargate Universe tiene previsto su estreno en Syfy el próximo otoño también. Y mientras, en la Comic-Con, que ha proporcionado numerosas novedades respecto a series, se han dado a conocer nuevas "promos" y posters de la misma.

Aunque Stargate Universe tiene dos predecesoras (Stargate Atlantis y Stargate SG-1), son numerosas las caras nuevas que nos encontraremos en esta ocasión. Pero también alguna entrañablemente conocida: Richard Dean Anderson, actor de la original Stargate-, ha hecho aparición en la "promo" especial mostrada en el evento. Los productores han anunciado, según se hace eco SpoilerTV.com, que el veterano volverá a aparecer en la serie. En ese mismo foro se hacen eco del parecido con BattleStar Galactica en cuanto a la temática (la tierra ha sido destruida, los humanos han huido) pero nos sorprenderá un nuevo nivel de comedia, avisan. <

Eureka consigue una cuarta temporada



Aunque en España haya pasado un poco desapercibida, cabe remarcar que esta serie de Syfy ha anunciado en la Comic-Con una cuarta temporada de 22 episodios. Protagonizada por Colin Ferguson, Salli Richadson-Whitfield, Joe Morton, Jordan Hinson, Edd Quin y Neil Grayston, entre otros, Eureka es una mezcla de comedia y ciencia ficción, pues la trama se sitúa en una ciudad ubicada en una remota área de la costa pacífica y que da nombre a la serie. En Eureka, población creada después de la Segunda Guerra Mundial, el gobierno americano ha estado recolocando a grandes genios, intelectuales y grandes pensadores y a sus familias. En este pintoresco lugar la vida diaria es una mezcla de innovación sin precedentes y caos total. Ninguna persona no autorizada puede saber de la ubicación del pueblo, pero el Oficial Jack Carter termina descubriéndolo cuando sufre un accidente con su coche y queda atrapado en el pueblo, junto a su hija. En España, la tercera temporada se emitió en SciFi, por lo que tal y como señalan en SeriesAdictos.com, la cuarta es de esperar que llegue en 2010. <

¿Otra retirada? ¿o publicidad?

Según ha hecho público Seth MacFarlane, creador de Padre de familia, la cadena Fox habría rechazado un nuevo episodio de la serie para el que previamente 20th Century Fox habría dado luz verde. El episodio pertenece a la próxima temporada y trataría sobre el aborto, según recoge Entertainment Weekly (www.ew.com).

Tal y como recuerda FórmulaTV.com, si finalmente el capítulo no se llegara a emitir sería la segunda vez que una entrega de Padre de familia es censurada por la cadena. Y es que en el año 2000, el episodio 'Cuando necesitas un judío' también fue retirado. Sin embargo posteriormente se incluyó el controvertido episodio en la edición en DVD de la serie. MacFarlane no descarta que suceda lo mismo con este episodio sobre el aborto. ¿Es una censura en toda regla o un reclamo publicitario? Últimamente se han dado algunos casos, y ahora nos referimos a cadenas españolas, que han usado estrategias basadas en la polémica y a los temas controvertidos para conseguir más audiencia. ¿Podría ser este un caso similar? Ciertamente no queda muy claro el tema... <





REVISTAS+WEBSITES+COMUNIDADES

MC EDICIONES S.A. www.mcediciones.com

Paseo San Gervasio, 16-20 - Tel. 93 254 12 50 - Fax 93 254 12 63 - 08022 Barcelona

Orense, 11 bajos - Tel. 91 417 04 83 - Fax 91 417 04 84 - 28020 Madrid



Náutica



www.revistagrandesesloras.com



www.larevistanautica.com



www.revistayate.com

Música











Hobbies y entretenimientos

























Literatura



Decoración













Viajes



Motor y Tuning



www.revistaautopasion.com



www.revistagti.com





www.revistasupervw.com





www.revistamundo4x4.com



www.revistamotoviva.com



www.revistamotott.com



www.revistavivascooter.com



www.revistamotosdeayer.com





Animales y Plantas









www.revistacaballo.com



Ciencia



www.masalladelaciencia.es

Arqueología e historia

Cocina















Estilo de vida



www.larevistaintegral.com

T.I.C. (tecnología de la información y comunicación)





www.revistatcn.com



Salud y deporte



www.revistamountainbike.com



www.revistaciclismoenruta.com

Videojuegos



Familia

Ahora en MC





Moda, salud y belleza







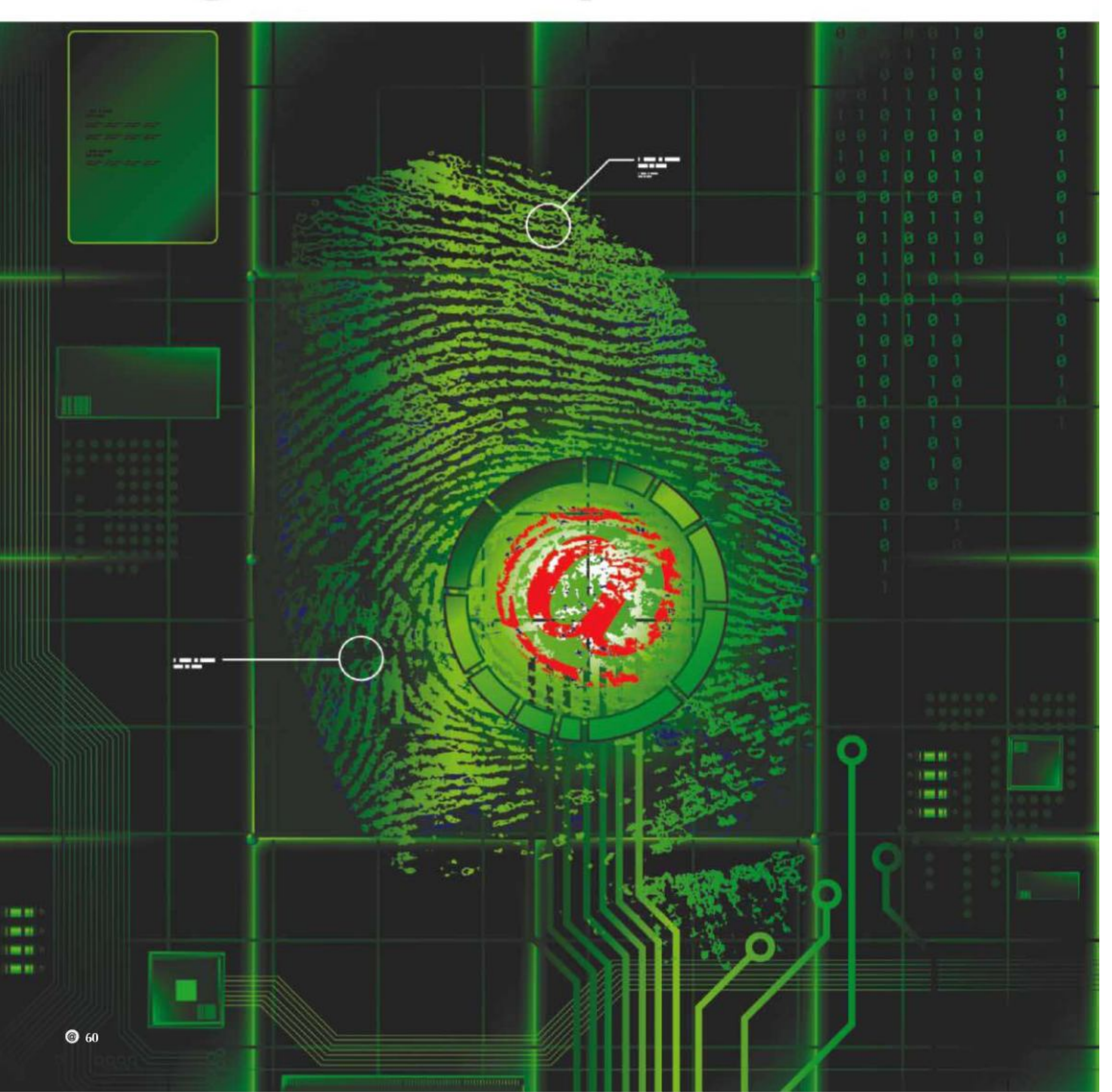


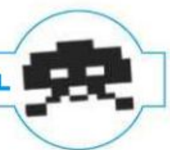
Creatividad Digital





Biometría:
la seguridad más personal





El primer requisito de cualquier sistema de seguridad que se pretenda eficiente es identificar a las personas. Si hasta ahora sólo se contaba con métodos arriesgados, como el DNI o las tarjetas de identificación, con la biometría ha nacido la primera tecnología capaz de responder sin vacilaciones a la espinosa pregunta del quién es quién: nuevos métodos de identificación que se basan en la huella dactilar, el iris o las inflexiones de la voz, es decir, en rasgos personales imposibles de suplantar.

La seguridad es aval de pervivencia y garantía de futuro para numerosos proyectos. De ahí que empresas, particulares e instituciones públicas se hayan preocupado siempre de salvaguardar datos privados e información confidencial, así como de controlar el acceso a sus domicilios e instalaciones. Ahora además, surgen peligros inéditos que reclaman métodos de protección más sofisticados: de una parte la proliferación de redes y sistemas informáticos aún vulnerables que abren nuevas vías de riesgo y, de otra, es necesario hacer frente a las amenazas propias de la sociedad globalizada, con el terrorismo como mayor exponente. No obstante, ante los nuevos retos nacen siempre nuevas respuestas, y así empresas, particulares e instituciones ya cuentan con una tecnología adaptada a los tiempos que corren: la biometría. Está basada en el reconocimiento de un rasgo corporal único en cada individuo, es decir, utiliza rasgos distintivos e inequívocos como las huellas dactilares, el iris del ojo o la palma de la mano para identificar a las personas. Esto significa que su principal característica es que identifica a las personas en función de quiénes son y no de lo que traen consigo como pueden ser tarjetas, llaves o credenciales, o de las que pueden recordar, como contraseñas o claves personales de autentificación.



Los atentados del 11 de septiembre en Nueva York supusieron el impulso definitivo para el desarrollo y la instalación de este tipo de sistemas, cada vez más frecuentes en aeropuertos, sedes empresariales y hasta en artículos de uso cotidiano, como ratones de ordenador, teclados o PDAs. El motivo es que organizaciones de de todo el mundo adquirieron una mayor conciencia de la importancia de la seguridad y comenzaron a reclamar soluciones más eficientes para salvaguardar el acceso a sus datos, garantizar cualquier tipo de transacción y proteger la entrada a sus instalaciones. Y la biometría pasó entonces a ocupar un papel protagonista, saliendo del lugar de exclusividad al que había estado recluida.

Como en una película de espías

Todas las técnicas biométricas se basan en el mismo esquema de funcionamiento: el sistema mide previamente una característica determinada del sujeto y la graba en forma de patrón numérico en su base de datos. Posteriormente, compara este patrón con el que presenta la persona que desea identificarse, ya sea para acceder al edificio, utilizar un dispositivo electrónico provisto de este sistema o, simplemente, acreditarse. La idea es la misma que en las antiguas películas de espías, donde las puertas reconocen al protagonista y se abren a su paso. Pero eso sí, la realidad es aún más rica y prolífica que un guión hollywoodiense ya que existen numerosas técnicas biométricas que utilizan distinta información y ofrecen resultados diversos según estén basadas en el iris, la firma manuscrita o la forma de la mano, por ejemplo. Los métodos más comunes son los clasificados dentro de la denominada biometría estática, es decir, aquellos que utilizan rasgos fisiológicos para realizar la autentificación:

· **Huella dactilar.** Es el método más extendido. De hecho, según el Grupo Internacional de Biometría (IBG, por sus siglas en inglés) representaba el 50,2% de los sistemas biométricos instalados en 2002. Se basa en el dibujo de la epidermis del dedo (generalmente el índice), cuyas crestas y surcos difieren en cada individuo. Cada huella contiene en sí misma tanta información que el sistema no memoriza más que ciertas irregularidades, como bifurcaciones o líneas que se pierden. Aunque cada dedo contiene alrededor de una centena de estos puntos clave, basta con utilizar doce de ellos para garantizar la autentificación, pues se considera estadísticamente imposible encontrar dos individuos en los que coincidan estas irregularidades. Además, el funcionamiento es sencillo: el usuario no tiene más que situar el dedo en un escáner para que se realice la lectura y el sistema verifica la identidad del individuo. La fiabilidad y la posibilidad de utilizar pequeños lectores que se integran fácilmente en todo tipo de dispositivos han propiciado el desarrollo y la gran aceptación de esta técnica. Sin embargo, no deja de presentar inconvenientes: cuando los dedos sufren alguna lesión o están sucios la lectura puede resultar dificultosa.



· **Forma de la mano.** En este caso la persona sitúa su mano abierta sobre un escáner específico y el sistema biométrico la reconoce a partir de la forma y geometría de la misma. La extensión de los dedos, la forma de las articulaciones y las dimensiones de cada falange son algunas de las características que se tienen en cuenta. Esta técnica goza de gran aceptación, sobre todo en los EE UU, y sus resultados suelen ser bastante buenos. Sin embargo, puede presentar errores de autentificación en caso de gemelos y personas de la misma familia.



· **Iris del ojo.** En los años ochenta los oftalmólogos se percataron de que, si bien el color del ojo puede variar dependiendo de la luz y la edad, no ocurre lo mismo con el dibujo que se representa en el iris. En efecto, cada ojo es único: las fotografías muestran alrededor de 200 variables independientes, de modo que resulta muy difícil confundir a dos individuos utilizando este patrón.

El usuario no tiene más que colocarse frente a una cámara que se encarga de escanear el iris para efectuar la comprobación. Como su dibujo no tiene relación con el código genético, el sistema es incluso capaz de distinguir gemelos. Sin embargo, se le puede engañar utilizando una fotografía o lentillas que reproduzcan el iris original. Por ello cada vez es más frecuente que estos sistemas incluyan medidas para asegurarse de que se trata de un ojo humano. Así, se varía la intensidad de la luz para comprobar que cambia de tamaño.

· **La retina.** Se trata de una de las técnicas de identificación biométrica más seguras que existen, aunque es muy mal aceptada por el público. Y es que para efectuar la medición es necesario iluminar el ojo, lo que provoca una sensación muy incomoda. En esta ocasión el sistema se basa en la diferente disposición de los vasos sanguíneos que recorren la retina dado que, aunque la edad o las enfermedades pueden modificar el aspecto, su posición relativa se mantiene siempre. El patrón almacenado puede contener hasta 400 puntos característicos del sujeto.



El otro tipo de métodos de identificación biométrica son los que se basan en características propias del comportamiento y están clasificados bajo el nombre genérico de biometría dinámica. En todos ellos el usuario debe realizar una determinada acción para que el sistema pueda identificarlo:

· **Reconocimiento de voz.** La voz es otro de los patrimonios únicos del individuo: como todos los sonidos, se caracteriza por la frecuencia, el tono y la intensidad, pero éstas varían en cada persona y, por tanto, resulta muy difícil de imitar. Con la ayuda de un micrófono el sistema almacena un patrón que atiende a estas diferencias y lo compara con las características de la voz del usuario a la hora de realizar la identificación. Eso sí, existen dos tipos de métodos, según se basen en frases predeterminadas o permitan a la persona hablar libremente. También varía la información analizada para el reconocimiento, que puede consistir en determinadas palabras o fonemas.

Entre las desventajas de esta técnica está la sensibilidad a los diferentes estados físicos o emocionales. Asimismo, el ruido ambiente puede dificultar el reconocimiento. Eso sí, se puede utilizar en las comunicaciones telefónicas por lo que es el único método hasta ahora que proporciona identificación biométrica a distancia.

· **Firma.** En este caso, el usuario debe firmar con un puntero electrónico sobre una tableta digitalizadora que analiza los resultados comparándolos con el patrón para efectuar la autentificación. El sistema se basa en la diferenciación de las partes cambiantes y aquellas que son habituales en la firma. Así, suele almacenar variables como la velocidad, las aceleraciones o la presión ejercida.

Aunque este tipo de biometría es aún poco utilizada, tiene la ventaja de permitir la identificación en documentos electrónicos o contratos y se espera que pronto prospere en estas aplicaciones específicas.

· **Teclado.** Se basa en la forma de trabajar con el teclado, concretamente se tiene en cuenta la dinámica de la presión ejercida: duración entre los golpes, duración del propio golpe o frecuencia de errores. El problema es que se trata de un comportamiento poco estable, ya que la forma de teclear puede variar según la naturaleza del texto y es bastante sensible al estado subjetivo de la persona.



Aún existen otros métodos de identificación biométrica, tanto estáticos como dinámicos, que o bien están muy poco extendidos, o bien continúan en fase experimental. Es el caso de la termografía, que se basa en obtener un cliché por infrarrojos del calor que desprende cada individuo y su distribución. A pesar de tratarse de un sistema muy preciso, resulta caro, por lo que su utilización es poco frecuente. También existen investigaciones sobre técnicas si cabe más sorprendentes, como las basadas en la forma de la dentadura, en el olor o en los latidos del corazón. En realidad, el único requisito para que una característica humana pueda servir para un proceso de identificación biométrica es que sea verdaderamente personal e insustituible. A partir de ahí, el tiempo terminará dictando cuáles son los métodos más cómodos y fiables para cada aplicación.

Ventajas y aplicaciones

Más allá de las investigaciones, aplicaciones y técnicas existentes, existe una razón fundamental que garantiza la evolución y creciente implantación de los sistemas de seguridad biométricos: la eficiencia. Y es que mientras el DNI, las contraseñas o las tarjetas de identificación son artículos independientes de la persona y pueden perderse, la biometría se basa en lo que ésta verdaderamente es: los rasgos corporales y del comportamiento no pueden extraviarse. De esta forma, una vez garantizada la identificación y minimizado el riesgo de fraude, se cierra el ciclo de la seguridad. Sin embargo, no sólo se trata de cumplir este objetivo sino de hacerlo de la forma más cómoda para el usuario.

Consciente de todas estas prestaciones, el Gobierno de los Estados Unidos se ha preocupado de fomentar el desarrollo de esta tecnología desde 1992. Ésta es la fecha en la que se inaugura el Consorcio Biométrico (Biometric Consortium), una red de investigación, desarrollo y experimentación. De hecho, las instituciones y

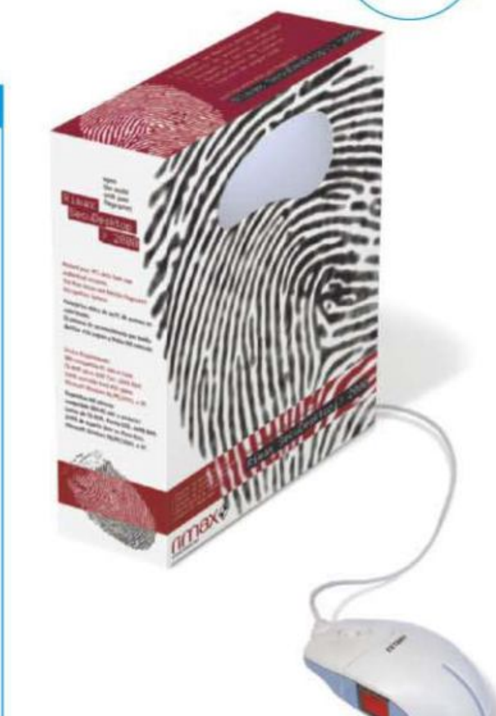
>>> DE CIENCIA FICCIÓN... O NO TANTO

La biometría no sólo es autentificación y seguridad, también es el embrión de los futuros sistemas de reconocimiento basados en emociones: cajeros, quioscos y hasta vallas publicitarias que, a la manera del mejor de los vendedores, reaccionan ante las expresiones faciales de sus clientes. Y no se trata de meras elucubraciones ni de una película de ciencia-ficción: la división Teradata de la multinacional NCR, el Integrated Media Systems Center con sede en Los Ángeles y la Universidad del Sur de California (EE UU) trabajan desde 1997 en el proyecto E-motions. Uno de los objetivos de esta ambiciosa iniciativa es dotar a los terminales de autoservicio de un sistema que parte del reconocimiento facial para identificar las emociones y, lo que es más, posteriormente calcular las posibles reacciones ante los estímulos. Ya se están probando las primeras aplicaciones en cajeros que permiten, por ejemplo, detectar si el usuario está entornando los ojos porque no puede ver bien las letras o porque el sol se está reflejando en la pantalla. A partir de ahí, el sistema reacciona readaptando el interfaz y las condiciones de visualización de la pantalla. Como si fuera humano. O casi.



>>> EL PODER DE LA HUELLA

Aunque no existe unanimidad sobre el sistema biométrico más seguro, sí la hay sobre cuál es el más asequible y utilizado en empresas e instituciones: la huella dactilar. De hecho, su utilización como seña de identidad personal es uno de los procedimientos más antiguos que existen, bien con fines artísticos o rituales, como lo han demostrado los hallazgos prehistóricos de impresiones de huellas en Nueva Escocia, o bien como estrategia para autentificar documentos mercantiles, como se hacía en la antigua Babilonia. Un médico persa del siglo XIV fue la primera persona que hizo referencia al hecho de que la huella dactilar era diferente en cada individuo. Sin embargo, no sería hasta el siglo XIX cuando el sobrino de Charles Darwin, el antropólogo Sir Francis Galton, realizara un profundo estudio de la huella dactilar con el objeto de buscar una metodología que sirviera para la identificación de los personas. Su método fue utilizado como prueba legal por primera vez en 1901 en Inglaterra, añadiéndole, eso sí, unas mejoras que hizo Sir Richard Henry, padre del método Henry, sistema que se utiliza aún en nuestros días para identificar a las personas por sus huellas dactilares. Esta larga trayectoria ha hecho posible que los dispositivos basados en el reconocimiento de la huella dactilar sean hoy día los más numerosos en el mercado. Según IDC, el 71% de los ingresos en biometría que se producen en Europa Occidental proceden de los dispositivos basados en esta tecnología. Una cuota que en el 2005 descenderá únicamente hasta al 67%. Unos de los últimos avances destinados a aumentar su fiabilidad ha venido con el sistema de reconocimiento dactilar por ultrasonidos. Ha sido desarrollado por la empresa valenciana Mundiscan (www.mundiscan.com) y se basa en el envío de ondas de ultrasonidos que rebotan sobre la base misma de la huella, lo que garantiza una seguridad cercana al 100% al no poder ser falsificada por ningún dibujo o material como el látex.



grandes eventos públicos han sido el primer escenario de prueba de estos sistemas. Es el caso de los Juegos Olímpicos de Salt Lake City, en 2002, donde se experimentó con un sistema de cámaras digitales que detectaban una serie de rasgos previamente programados. También existen ejemplos de proyectos públicos en nuestro país. Unisys ha implantado una solución piloto para el reconocimiento de los afiliados al INEM por medio de la huella. Pero donde más ha proliferado la seguridad biométrica ha sido en los aeropuertos. Así, desde octubre de 2001, el Shiphol de Amsterdan (Holanda) emplea un novedoso e instantáneo sistema de control de embarque: el escaneo del iris. Este sofisticado procedimiento de seguridad tiene dos fases. En una primera (que dura unos 15 minutos), el viajero es clasificado y registrado, para lo que, además de revisar su pasaporte y pasar un control rutinario, se le escanea el iris del ojo. Los datos son encriptados e insertados en una tarjeta inteligente. En una segunda fase, que dura alrededor de unos quince segundos, se identifica y confirma la identidad del pasajero registrado en la zona de embarque. Para realizarla, inserta la tarjeta en el lector y mira fijamente a una cámara para un segundo escaneo del iris. Si los datos biométricos concuerdan con los datos de la tarjeta, el viajero podrá continuar su camino. De lo contrario no se le permite la entrada y debe pasar un segundo control policial de pasaportes.

Pero los sistemas biométricos tampoco han tardado en dar el salto a la empresa y el hogar. En el año 2000, Argentaria (en la actualidad BBVA) fue pionera en la utilización de un cajero automático de la compañía NCR que incorporaba un sistema de reconocimiento del iris que sustituía a la tradicional identificación basada en el número secreto o PIN. El sistema fotografiaba el ojo y transformaba la imagen en dígitos que, una vez convertidos en un código, se comparaba con los datos almacenados en el archivo y confirmaba si el usuario era o no el propietario de la tarjeta. Otro ejemplo es el sotware de control de presencia mediante huella dactilar en las empresas, como Staff Control del Grupo CDW o Morpho Acess de Sagem. Pero no todo se queda en el control de accesos: cada vez más dispositivos electrónicos incorporan sistemas biométricos para identificar a su dueño: smartphones, portátiles, periféricos informáticos.... No sería de extrañar, por tanto, que en los próximos años los dispositivos biométricos serán tan utilizados como las tarjetas bancarias que hoy en día todos utilizamos







¿Está seguro nuestro portátil o móvil?

Con el objetivo de responder a los cada vez más frecuentes requisitos de movilidad de los trabajadores, las empresas extienden sus redes corporativas a pesar de los riesgos que ello implica. Para hacer frente a la infinidad de amenazas existente están surgiendo nuevos enfoques en seguridad basados en políticas capaces de mantener la información a salvo y de sellar todos los puntos susceptibles de convertirse en un 'agujero negro'.





Seguridad en dispositivos móviles

Si hay una tendencia de la que se habla sin parar en los entornos empresariales es de la necesidad de expandirse geográficamente y facilitar la movilidad laboral.

No en vano, según un estudio de IDC, en España existen actualmente más de ocho millones de trabajadores móviles, situándose a la cabeza de Europa y por delante de países como Francia, Reino Unido, Alemania e Italia.

Las posibilidades de conexión, la capacidad de procesamiento y las limitaciones de sistemas operativos y aplicaciones eran algunos de los obstáculos que frenaban la expansión de estos dispositivos.

Cada vez más superados, gran parte de la información de muchos negocios está ya en terminales móviles –desde portátiles a smatphones o PDAs-, por lo que su seguridad debe ser tenida muy en cuenta. Este tipo de dispositivos pueden estar durante días fuera de las 'murallas' seguras de la oficina, con miles de riesgos acechándoles.

A menudo nos podemos encontrar con que el puesto de usuario funciona, pero simplemente no sabemos utilizarlo; que tenemos una duda sobre la última sincronización de los datos recibidos o sobre la utilización de una determinada función de la aplicación; que tenemos un error de conexión a la red o de sincronización de los datos.

También es posible que el dispositivo móvil no funcione. Por todo ello nos gustaría disponer de un Servicio telefónico de soporte también desde cualquier lugar en cualquier momento.

Las diferentes tecnologías de dispositivos móviles mencionados en apartados anteriores, el entorno cambiante de las mismas y la integración de éstas con el resto de la infraestructura asociada a los procesos de negocio, hacen que los usuarios que las utilizan precisen a menudo de necesidades de soporte como las mencionadas anteriormente.

El tipo de entorno en el que se encuentran habitualmente las personas que requieren este tipo de soporte (desde cualquier lugar, sin mesa, silla y otras comodidades), y el poco tiempo de disponibilidad (taxi, aeropuerto, entre reuniones, etc), requieren de una ayuda fácilmente accesible en un corto instante de tiempo, con una alta especialización del personal en la administración de los dispositivos y la disponibilidad de herramientas que permitan al personal de soporte resolver remotamente las incidencias y consultas planteadas por los usuarios.

LOS HACKERS TAMIBÉN ESTÁN EMPEZANDO A ESPECIALIZARSE, SIENDO BUEN EJEMPLO DE ELLO EL GUSANO 'CABIR', EL VIRUS 'COMMWARRIOR' O TROYANOS COMO 'SCULL'. EN ESTO CONTEXTO, LOS ATAQUES BASADOS EN LA USURPACIÓN DE IDENTIDADES Y CONTRASEÑAS ESTÁN EN AUGE DE FORMA ESPECIAL

Así pues, y dependiendo de la criticidad del soporte a los usuarios móviles en el caso de una interrupción, es muy importante que las organizaciones tengan en cuenta para la elección de la tecnología móvil, como un factor de decisión más, la capacidad de los dispositivos de ser controlados desde los centros de soporte con herramientas de control remoto que permitan a los agentes telefónicos conectarse al dispositivo y resolver la incidencia o adoctrinar al usuario según las consultas requeridas. Por otra parte, y para las incidencias que no puedan ser resueltas desde el centro telefónico, por ejemplo un sistema corrupto que impide la utilización del control remoto, o bien una avería en el material hardware que requiera de una sustitución rápida del dispositivo móvil, el centro de soporte deberá contar con un stock previsto de dispositivos destinados a reemplazar los averiados, y minimizar con ello el tiempo de interrupción de los usuarios que los utilizan.

Las crecientes demandas de acceso a la información desde cualquier lugar, en cualquier momento y desde cualquier dispositivo (portátil, PDA, teléfono móvil) para cumplir con las necesidades de los procesos de negocio de las compañías, implica el tener en cuenta tanto la infraestructura de las tecnologías de la información asociadas a todo el proceso de negocio (sistemas, comunicaciones y dispositivos) como al nivel de calidad que se precisa ante posibles caídas de servicio o degradaciones del mismo. Para cubrir dichas necesidades precisamos disponer de la mejor tecnología en cada momento, de los servicios de gestión y de soporte sobre la infraestructura y de una organización adecuada que permitan evolucionar la globalidad del proceso según las necesidades cambiantes del negocio de las compañías, y que aseguren a su vez la evolución tecnológica de los componentes de los sistemas de información asociados.

En caso de ser víctimas de cualquier tipo de malware, las consecuencias serían graves, ya que en ellos suele almacenarse información estratégica y de enorme valor.

Pero aún resultaría más trágico si el equipo infectado volviera a conectarse a la red corporativa y extendiera de forma involuntaria el código malicioso al resto de equipos.

Las amenazas que afectan a los dispositivos móviles no son sustancialmente diferentes de aquellas que acechan a las redes fijas, pero con un acceso a la red, en ocasiones, más sencillo debido a que hay más puertas abiertas y menos controles.

Además, los hackers están comenzando a especializarse, siendo buen ejemplo de ello el gusano 'Cabir', el virus 'Commwarrior' o troyanos como 'Scull'. En esto contexto, los ataques basados en la usurpación de identidades y contraseñas están en auge de forma especial ya que los dispositivos móviles son un blanco perfecto para los hackers, que persiguen capturar información con la que obtener ingresos ilícitos (Mophophising) o enviar e-mails de forma masiva (SpamMovile), hacer llamadas gratis o espiar al usuario.

La exposición a este tipo de amenazas no para de crecer por la expansión del teletrabajo y la adopción de las WLAN,

>>> FIRMA DIGITAL MÓVIL, ¿LA SOLUCIÓN DEFINITIVA?

Una de las tecnologías que más expectativas ha suscitado en los últimos tiempos es la firma digital móvil, en la que muchos ven uno de los sistemas más fiables para securizar las comunicaciones inalámbricas.

Sin duda, se trata de una opción altamente recomendable, pues es uno de los sistemas de autenticación más eficaces, y su implantación no tiene por qué resultar especialmente costosa.

Sin embargo, otras voces advierten de que por sí misma no garantiza la seguridad ni es capaz de hacer frente a todas las amenazas, por lo que resulta vital complementarla con otras medidas que aseguren el acceso. No hay duda de que la la firma digital de contenidos supondrá un gran avance en la protección de las plataformas móviles y, además, con el DNI digital se mejorará y complementará la identificación del usuario, pues la e-firma permite corroborar la autenticidad e integridad de la información que proporciona.



SEGÚN UN INFORME DE TREND-MICRO, CUANTA MÁS MOVILIDAD TENGA EL TRABAJADOR, MÁS INFORMACIÓN CONFIDENCIAL ENVÍA A TRAVÉS DE DISPOSITIVOS PORTÁTILES COMO SU MÓVIL O SU ORDENADOR PORTÁTIL.

por lo que los usuarios deben prepararse para un aumento de las 'agresiones' contra sus dispositivos portátiles.

Retos y prioridades

Según un informe de TrendMicro, cuanta más movilidad tenga el trabajador, más información confidencial envía a través de dispositivos portátiles. Su uso obliga a implementar dentro de su red sistemas que les permitan soportar la movilidad sin que se produzcan agujeros en su seguridad. Evitar que la información caiga en poder de quien no debe es el principal reto al que se enfrentan, por lo que resulta fundamental saber quién, cómo, para qué y cuándo se accede a los datos almacenados. Es decir, hay que dar respuesta a dos necesidades: las del usuario final, que quiere un dispositivo fácil de utilizar y fiable, y las del responsable de TI, que ha de tener centralizado el control de su sistema para reaccionar ante cualquier amenaza.

Dicho de otro modo, hay que garantizar el justo equilibrio entre un nivel adecuado de seguridad y un grado elevado de usabilidad. Se podrían desconectar los dispositivos de cualquier red de voz o datos, lo que garantiza protección, pero la solución se convertiría en algo completamente inservible. Además, los problemas los provocan, en gran medida, los propios empleados, debido a su falta de conocimiento y errores. No basta con confiar en que los usuarios aplicarán el sentido común y actuarán responsablemente: cada organización tiene que crear un entorno en el que la seguridad se perciba como algo natural e intrínseco.

Los fabricantes están desarrollando hardware y software específicamente diseñados para mejorar la seguridad de las aplicaciones y equipos móviles, pero los ataques también son cada vez más sofisticados. Por eso, lo más importante es definir una política que vaya más allá de 'capar' el acceso a recursos como el correo electrónico, Internet, la mensajería instantánea o los dispositivos extraíbles. No hay que olvidar que los hackers están continuamente escuchando las comunicaciones que se producen a través de redes ina-



lámbricas para encontrar potenciales vías de entrada. Y que la principal amenaza es siempre un usuario confiado o desconocedor de las reglas del juego. Por eso, resulta básico que las empresas sean conscientes de la importancia de 'blindar' los dispositivos móviles y que eduquen, formen e involucren a sus empleados. Sin embargo, no parece que se haya avanzado demasiado al respecto ya que depende en gran medida del tipo de empresa y de la actividad que se realice; no es lo mismo usar el equipo sólo como teléfono que como una oficina móvil.

Soluciones

Cualquier solución de seguridad que se adopte debe contemplar a los usuarios móviles y a las delegaciones remotas, pues en caso contrario, no es segura y se convierte en una brecha a través de la cual el malware puede hacer de las suyas. La mejor opción es decantarse por una gestión centralizada y simplificada de todo lo relacionado con la red, abarcando la seguridad desde diversos frentes: no hay que limitarse exclusivamente al perímetro o a la protección interna, y se debe apostar también por tecnologías como la autenticación, el cifrado o la recuperación ante desastres. Una opción viable son las soluciones anti-malware combinadas con un firewall que filtre las comunicaciones hacia/desde el dispositivo móvil. También es recomendable cifrar la información para protegerla en caso de pérdida o sustracción del terminal.

Pero la seguridad móvil no se sustenta únicamente en una solución de software, sino que los propios dispositivos deben implementar herramientas para proteger los datos que contienen, reciben y transmiten.

Los sistemas de identificación y control de acceso están evolucionando desde el mundo analógico al digital, y tecnologías como la detección del iris y de las huellas dactilares juegan un papel cada vez más relevante junto a las tradicionales tarjetas de contraseña y tokens. Conforme la biometría vaya avanzando y los precios sean más asequibles, estas tecnologías se irán integrando de forma nativa en los dispositivos móviles.

El reconocimiento dactilar, de iris o mediante el ADN son herramientas que se complementan a la perfección con el software de seguridad, ya que estas tecnologías garantizan la seguridad de acceso a los dispositivos y dificultan su uso por personas no autorizadas al añadir una capa personal e intransferible.



LOS HACKERS TAMBIÉN ESTÁN EMPEZANDO A ESPECIALIZARSE, SIENDO BUEN EJEMPLO DE ELLO EL GUSANO 'CABIR', EL VIRUS 'COMMWARRIOR' O TROYANOS COMO 'SCULL'. EN ESTO CONTEXTO, LOS ATAQUES BASADOS EN LA USURPACIÓN DE IDENTIDADES Y CONTRASEÑAS ESTÁN EN AUGE DE FORMA ESPECIAL

Beneficios tangibles

Los dispositivos móviles proporcionan una mayor productividad, mejor acceso a los datos y operaciones más eficientes, pero la contrapartida es el riesgo de que se produzca un acceso no autorizado a información empresarial importante, por lo que conviene tomar con estos aparatos las mismas precauciones que se adoptan con un equipo de sobremesa.

Una protección completa en todos los puntos de entrada reduce el riesgo de infecciones de la red corporativa, además de reducir el tiempo de no disponibilidad de los dispositivos y de los trabajadores que hacen uso de ellos.

Asimismo, se minimizan las incidencias de robo de información y las problemáticas en torno a la confidencialidad de los datos por la pérdida del portátil, la PDA o el smartphone.

Las ventajas son múltiples, pero pueden resumirse en una, y es que se evita perder información sensible, confidencial y crítica para la empresa.

Un futuro inquietante

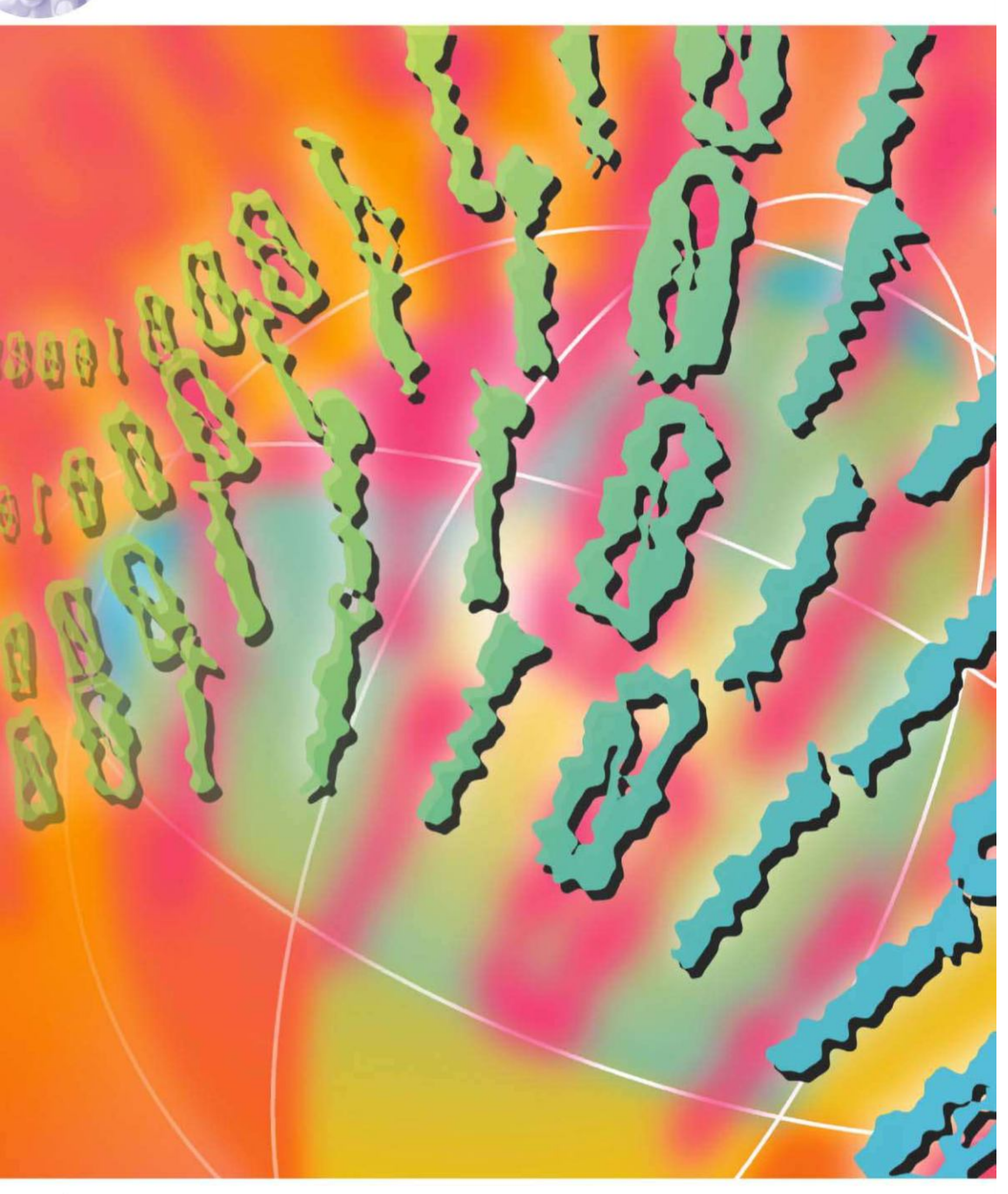
La expansión de los sistemas, las redes y los dispositivos móviles permiten llevarse la oficina a todas partes, y también que se multipliquen las amenazas. A medida que ganan en popularidad, se hacen más atractivas para los piratas informáticos.

Su introducción masiva representa uno de los retos tecnológicos más críticos actualmente, y lo continuará siendo a lo largo de los próximos años.

Con la aparición de malware específico para dispositivos móviles, es evidente que éstos requieren una protección adecuada y que la industria deberá evolucionar a la par que lo hacen las amenazas. Es probable que el futuro pase por soluciones globales, ya que se ha demostrado que a medio y largo plazo son mucho más rentables y estables.

Los operadores ya ofertan soluciones que abarcan desde la protección perimetral y de los sistemas hasta la consultoría, la autenticación del usuario u otros servicios, como la firma digital.

De lo que no parece haber dudas es que los riesgos para los dispositivos móviles se van a incrementar de forma exponencial en los próximos años, debido fundamentalmente a la combinación entre telefonía móvil, informática y telecomunicaciones.



Información encriptada, datos seguros

La encriptación se está convirtiendo en una medida de protección imprescindible en cualquier organización que desee tener su información a buen recaudo, sobre todo si los datos viajan por la Red.

Las redes han evolucionado desde los tradicionales sistemas cerrados hasta aquellos cada vez más expandidos que permiten conectar a partners, proveedores, clientes, teletrabajadores y usuarios inalámbricos. De ahí que las organizaciones tengan que afrontar con solvencia el hecho de que existe una infinita variedad de ataques agresivos y maliciosos capaces de comprometer sus datos y sus usuarios. Se descubren nuevas amenazas prácticamente a diario, y a medida que varía la naturaleza y el volumen del tráfico en Internet, también debe adaptarse el tipo de medidas que toman las empresas para asegurar la información y las comunicaciones de sus redes.

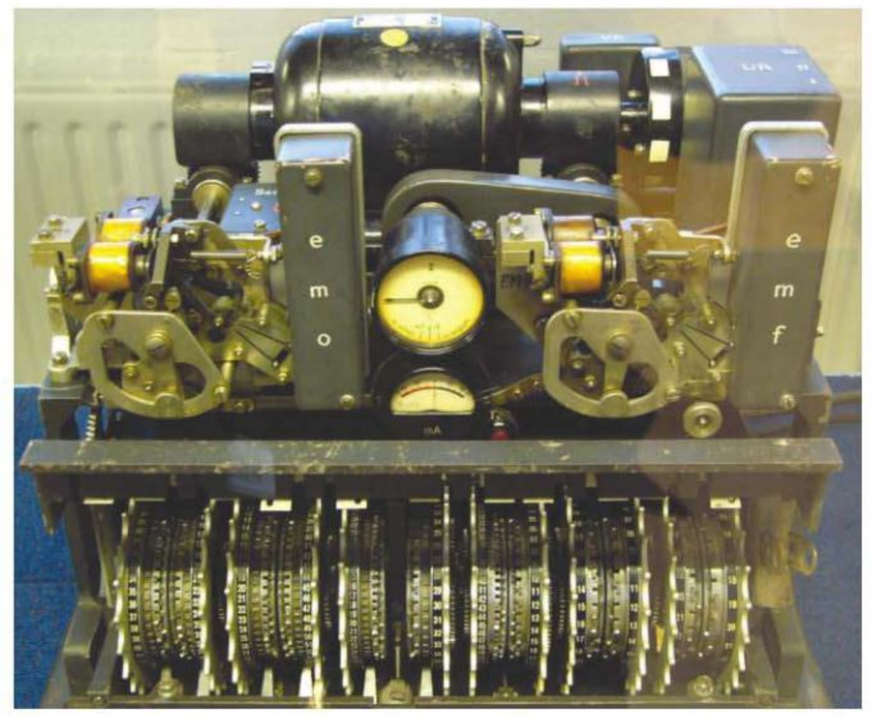
Cualquier dato que se pueda utilizar para identificar a un individuo, grupo, empresa o entidad debe estar estrictamente protegido ante accesos no autorizados desde su origen hasta su almacenamiento, especialmente si se envía o transmite por algún medio, sea éste cual sea. Y aquí es donde entra en acción la encriptación, que se ha convertido en una de las vías de almacenamiento, compartición y transmisión de datos más segura del mercado y que, básicamente, se trata del proceso mediante el cual cierta información es cifrada de forma que el resultado sea ilegible a menos que se sepa interpretar.

Más en concreto, la encriptación, ya sea software o hardware, es la tecnología para cifrar mensajes de correo electrónico, archivos de bases de datos y otra información con el fin de mantenerlos confidenciales. Mediante el uso de ecuaciones matemáticas sofisticadas, posibilita la protección de la información confidencial con una 'cerradura electrónica' que impide a ladrones y hackers obtener datos privados o personales.

Fines militares

En un primer momento, la encriptación se destinó exclusivamente al ámbito de las agencias de inteligencia y con fines militares. Con la irrupción de las nuevas tecnologías, comenzó a evolucionar dando paso a los sistemas actuales. Hoy en día, se han elaborado una serie de algoritmos que permiten codificar la información haciéndola prácticamente indescifrable, puesto que simplemente con claves de 128 bits un ordenador tardaría 200 millones de años en conseguirlo.

Con el auge de la tecnología informática y el uso de redes para compartir la información y hacer negocios, se ha convertido en una parte fundamental de la estrategia de seguridad de cualquier empresa. Así, las soluciones de encriptación pueden proteger información financiera y médica de carácter confidencial contra su divulgación no autorizada, salvaguardar las transacciones de comercio electrónico –incluyendo los números de las tarjetas de crédito-, mantener la con-



La máquina alemana de cifrado Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes para los generales de muy alto rango.



La máquina Enigma utilizada por los alemanes durante la II Guerra Mundial.

fidencialidad de los negocios y ayudar a que en una transacción ambas partes autentifiquen la identidad de la otra.

¿Cómo funciona?

Las herramientas de encriptación utilizan operaciones matemáticas complejas para intercambiar información confidencial entre dos partes que se conectan a través de una red insegura como es Internet. En la World Wide Web no tenemos conocimiento ni control del camino que siguen nuestros datos hasta llegar a su destino, por lo que técnicamente es posible interceptar una comunicación, 'escuchar' lo que se dice o incluso alterarla. Los métodos criptográficos tradicionales operan a partir de una palabra o frase llave, el conocido password, que sirve para codificar y descodificar información. Su punto débil es precisamente el proceso de difusión, dado que la llave debe ser conocida por los dos extremos de la comunicación. Por el contrario, la criptografía de clave pública asigna a cada parte una par de llaves, una pública que cualquiera puede conocer, y otra privada que es fundamental para garantizar la seguridad.

Para enviar un mensaje, se codifica con la clave pública del usuario y se genera una 'firma digital' del mismo. El sistema garantiza que el mensaje resultante sólo puede ser descodificado con la clave privada. Ese certificado digital es el equivalente al DNI y asegura la correspondencia entre la identidad de un usuario o servidor y su correspondiente clave pública.

Un mercado en auge

Conceptos como virus, gusano, hacking o robo de identidad forman parte de la informática común. Como resultado, la seguridad de nuestros datos personales

>>> LOS MECANISMOS MÁS COMUNES DE ENCRIPTACIÓN

• IPSec (Seguridad del Protocolo de Internet). Garantiza la confidencialidad e integridad de los paquetes IP. Protege y blinda el tráfico y la información de la aplicación durante la comunicación. Suele emplearse para construir una relación de confianza entre servidores al crear redes privadas virtuales (VPN).

• SSL (Secure Sockets Layer). Es el método de protección más utilizado, al usarse en aplicaciones de correo electrónico y web, como las conexiones con la banca online. Viene incorporado en los navegadores de Internet más habituales y autentifica la identidad de las partes, asegura que la información se transmite de forma confidencial y mantiene la integridad de los datos transmitidos.

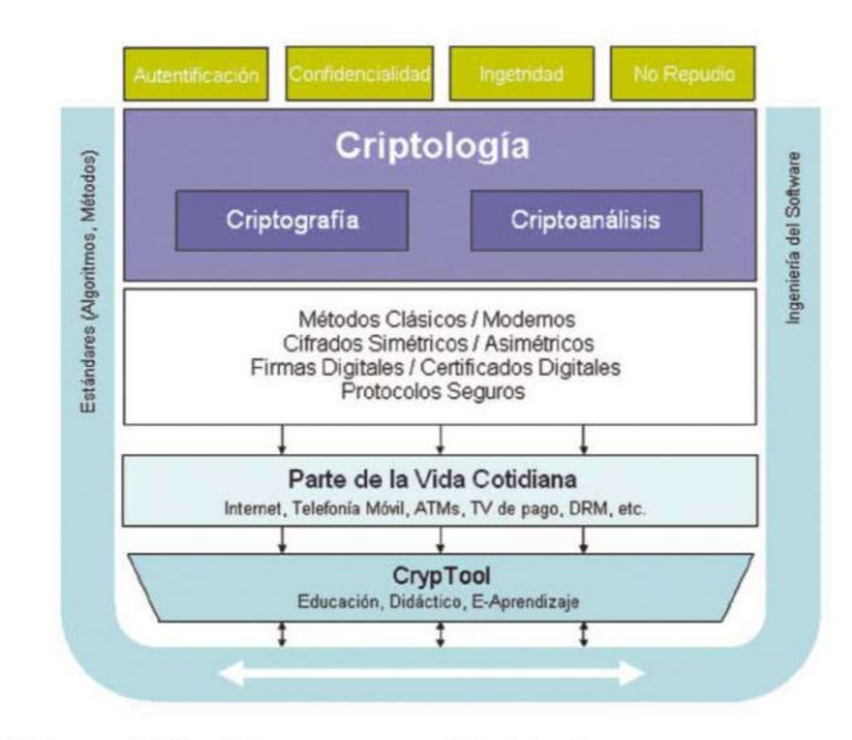
• SSH (Secure Shell). Apropiarse de una contraseña a partir de una conexión Telnet es relativamente fácil para los piratas, y la mejor manera de evitarlo es mediante SSH, que se basa en algoritmos de encriptación de alto nivel y en el uso de múltiples y sólidos métodos de certificación de claves públicas.

• VPN (Red Privada Virtual). Se suelen utilizar cuando las LAN se han conectado mediante una red no fiable. La conexión se hace mediante algo parecido a un túnel protegido, por ejemplo, entre la central de una empresa y una sucursal.

• PGP (Pretty Good Privacy) y S/MIME. Son los dos sistemas más utilizados para la encriptación de mensajes de correo electrónico. PGP es el más usado y se emplea para proteger los archivos de los usuarios, así como para enviar y recibir mensajes confidenciales y sus respectivos adjuntos, que se certifican con una firma digital. En cuanto a S/MIME, utiliza básicamente los mismos algoritmos que PGP y la principal diferencia es que requiere un código digital que concede un organismo certificador externo, por lo que se trata ante todo de una aplicación comercial.

se ha convertido en el mayor reto al que se enfrentan los administradores de sistemas en estos momentos. En este sentido, las técnicas de encriptación están demostrando ser las más efectivas para combatir estas amenazas, por lo que el futuro de este mercado es prometedor, tanto a nivel mundial como en el caso de España. En nuestro país, el mercado de la encriptación se está homogeneizando poco a poco, sobre todo a raíz del desarrollo de las comunicaciones móviles corporativas.

En cuanto a las tecnologías imperantes en esta área de la seguridad informática, no cabe duda de que ahora se habla mucho de WEP, WPA o VPN (redes privadas virtuales) debido al enorme desarrollo que están experimentando las redes WLAN, aunque no por ello deben olvidarse el resto de componentes de la red. Por el lado de la seguridad perimetral destaca el cifrado entre diferentes sedes, de obligada integración por ley, mientras que si hablamos de seguridad interna, hay que mencionar la encriptación de discos, dispositivos, e-mails o backups.



Visión general de los objetivos y componentes de la criptografía

Una buena estrategia, imprescindible

La posibilidad de sufrir pérdidas de la información almacenada electrónicamente crece exponencialmente, y la culpa no es sólo de los hackers o de empleados negligentes, sino que recae fundamentalmente en los negocios que no consiguieron encriptar sus datos confidenciales. El fracaso a la hora de protegerlos no es sólo una amenaza para los clientes, sino que también pone en peligro la reputación de la empresa y, en algunos casos, puede incluso llegar a ser hasta un delito.

Por ello, resulta fundamental definir una estrategia de encriptación eficaz, que contemple tanto la seguridad externa como la interna. Las organizaciones han de planificar su seguridad de modo global, analizando qué tipo de conexiones se establecen y qué tipo de información es la que se quiere proteger. No hay una única solución de encriptación capaz de proteger todas las áreas de datos. Según el Instituto Nacional de Estándares y Tecnologías (NIST), existen varias herramientas criptográficas, que se dividen en cinco categorías principales: a nivel de archivo o carpeta, volumen o partición, multimedia, de campo y comunicaciones. Las posibilidades son múltiples, e incluso resulta difícil conocerlas todas. Su eficacia depende en parte de las necesidades de la empresa, puesto que no a todas les va a resultar útil la misma solución. Sin embargo, las técnicas de cifrado más eficaces siempre serán las que se apoyan en estándares, como pueden ser IPSec y VPN_SSL, compatibles con todas las tecnologías del sector.



¿Hardware o software?

Hasta hace bien poco, la seguridad de nuestros datos sólo se protegía vía software, de modo que si nos robaban el disco duro o hacían una copia de él, se podía llegar a desencriptar toda la información que contenía. Es por ello que la industria está apostando fuerte por la encriptación vía hardware, que trabaja directamente sobre el disco y viene integrada en el mismo, sin necesidad de instalar ningún tipo de software adicional o adquirir caros programas propietarios. Ante este panorama, a las empresas se les presenta la tesitura de por qué tecnología apostar. El hecho de utilizar encriptación vía software implica un bajo coste y mayor flexibilidad, aunque es más lento y vulnerable. El hardware aporta mayor rapidez y seguridad, pero por contra resulta más caro y menos adaptable. Lo mejor es elegir una combinación de ambos ya que disponer de un potente algoritmo no es suficiente, pues si se llega a desvelar la llave, el sistema queda completamente vulnerable a los ataques de los hackers.

La evolución de este área de la seguridad informática no se va a detener, por la sencilla razón de que los 'malos' no dejan de pergeñar nuevas amenazas con las que asaltar los sistemas. Además, ya no se parecen en nada a aquellos virus cuyos creadores sólo buscaban notoriedad, sino que su intención es obtener algo más, que no es otra cosa que un beneficio económico. No cabe duda de que ningún particular o empresa debe bajar las defensas, por lo que si hay un mercado dinámico ése es el de la seguridad.

>>> SEGURIDAD MÓVIL

Los dispositivos portátiles se han convertido en el objeto de deseo de los 'piratas', por lo que resulta fundamental la integración de herramientas de encriptación que hagan frente a estas amenazas. Las soluciones de encriptación están resultando fundamentales en el desarrollo de las soluciones móviles y los dispositivos inalámbricos al permitir establecer y mantener conexiones seguras conservando la transparencia en las comunicaciones. Si no hubieran existido estas medidas de seguridad, las empresas no hubieran podido desarrollar una infraestructura de redes móviles, y esto es más evidente aún desde la incorporación de la voz a las redes VoWLAN.

Soluciones IPS: protección global

Ante la decepción provocada por los sistemas de detección de intrusos, las soluciones IPS se presentan como la alternativa de futuro en materia de seguridad interna. Los IPS recogen los datos que llegan de cortafuegos, servidores y otros focos y proporcionan respuestas integradas sobre lo que está pasando en las redes, tanto los intentos de ataque, o malware, como la manera de solucionar problemas detectados. Actúan, por tanto, de manera proactiva e integradora: ahí está la clave de su éxito en un ambiente en el que la seguridad resulta básica para hacer frente a un número cada vez mayor de ataques.

El manejo cada vez mayor de información (voz, vídeo y audio) a través de redes (internas o externas) ha traído consigo el incremento de las amenazas en las vías de comunicación de muchas empresas y, como consecuencia, la imperiosa necesidad de protegerse ante cualquier tipo de vulnerabilidad que afecte a estos canales. Ante esta situación, los sistemas de protección perimetral resultaban incapaces de solventar totalmente los ataques ya que limitaban su funcionamiento a establecer una frontera que permitiera o denegara, en base a unos perfiles, el acceso de los datos a las redes. Estas herramientas no conseguían detectar el contenido de esa comunicación, de manera que desechaban o admitían informaciones que no siempre eran perjudiciales o beneficiosas, según los casos.

Como consecuencia de esta carencia en los cortafuegos, a finales de los 90 salieron al mercado los IDS (Intrusion Detection Systems) o sistemas de detección de intrusos, que proporcionaban un paso más en las tareas de seguridad de redes: no sólo marcaban protocolos para el tráfico de información (como los firewall), también examinaban esa transmisión que se efectuaba en una red interna (entre los PCs de una oficina, DMZ y red...) discerniendo lo que era una comunicación limpia de una infectada. No obstante, tampoco las tecnologías de detección de anomalías dieron los resultados que se esperaban, ya que para asegurar el éxito requerían una gran cantidad de técnicos especializados en analizar e interpretar las alarmas enviadas por los sistemas de detección. Al final se producían tal cantidad de alertas que resultaba complicado descifrar lo que había sido un ataque de lo que no, enviándose en muchos casos falsos positivos. Además, los avisos se proporcionaban a posteriori, cuando la intrusión ya se había producido: detectaban un ataque pero no lo frenaban.

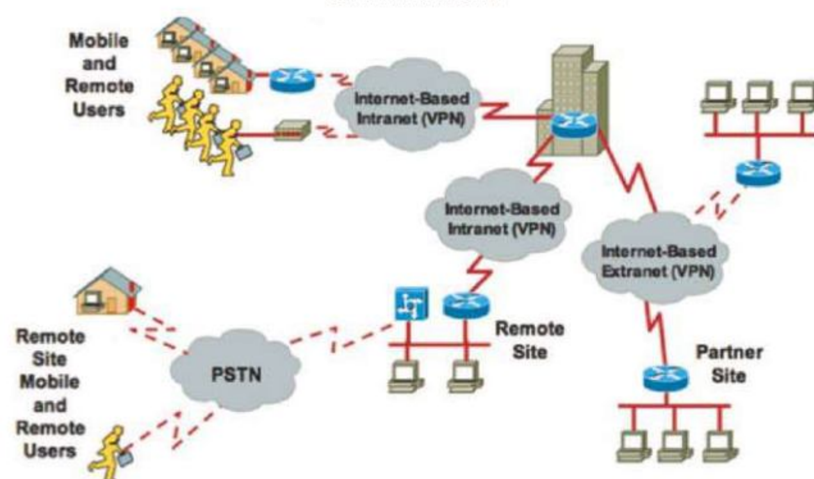
CUADRANTE MÁGICO DE GARTNER



Source: Gartner (February 2008)

Posicionamiento de las soluciones IPS según el Cuadrante Mágico de Gartner

OPEN NETWORK



Arquitectura IPS

Consecuencia del escepticismo provocado, de un lado, por el fracaso de la detección precoz y, de otro, por la necesidad de una cantidad enorme de efectivos, los IDS fueron evolucionando hacia soluciones proactivas que, además de distinguir los patrones de ataque y de diferenciar el tráfico limpio del dañino, entraban en colaboración con distintos mecanismos con el objetivo de tomar medidas para frenar una agresión. Pero para llegar a este punto fue necesario que se desarrollara una coyuntura propicia, por lo que los IDS evolucionaron hacia los conocidos como IPS (Intrusión Prevention Systems) o sistemas de prevención de intrusiones, dispositivos in line más próximos en su concepción a los firewalls tradicionales que, además de monitorizar, eran capaces de bloquear el tráfico indeseado.

Arquitectura global de seguridad

Las actuales soluciones IPS aprendieron del fracaso de los sistemas precursores de detección para definir con claridad las necesidades de seguridad que había que cubrir y las características que debían cumplir. El resultado de este proceso de revisión dio lugar a mecanismos proactivos frente a las intrusiones capaces de prevenir el ataque antes de que se produzca y de dar una respuesta global al mismo. Estos mecanismos analizan el contexto, es decir, examinan los distintos paquetes de información provenientes de otros sistemas de seguridad de una empresa, como firewall o servidores, y correlacionan todos esos datos depurándolos, de tal manera que no sólo evitan un trabajo extra al administrador por una falsa alerta, es decir, un menor consumo de recursos, si no que proporcionan una información más completa, precisa y en tiempo real. La palabra clave es correlación: correlacionar los eventos de distintas fuentes de información para analizar en profundidad si la información procedente de diversos puntos al final es susceptible de constituirse en un ataque o es simplemente un intento que no va a ser capaz de progresar.

Principales amenazas

Robo y destrucción de información, negación o parada de servicio a causa del envío masivo de conexiones contra una máquina, intentos fraudulentos de entrar en las redes, caídas de sistemas, gusanos y virus que se expanden por equipos vulnerables o servidores no parcheados a la última. En la actualidad, se producen los más variados ataques a la seguridad de las empresas y los sistemas IPS los combaten con un análisis en profundidad. No obstante, uno de los principales peligros se encuentra en el tráfico interno de una empresa. Proteger esta red es tan importante como marcar fronteras a través de cortafuegos. El desconocimiento por parte de las compañías del tipo de tráfico que está pasando por su red interna puede entrañar amenazas potenciales. Así, es muy común en las empresas que no se sepa por qué los sistemas van tan mal o por qué la red va tan lenta, debido a que no tienen controlado el tráfico interno y puede ser que los empleados estén utilizando el ancho de banda para descargarse películas, música o vídeos. Y es que muchas de las amenazas pueden provenir desde dentro de la organización debido a que usuarios usan herramientas sin tener en cuenta el riesgo que puede conllevar su utilización. Otra nivel de amenaza se centra en la protección de



Ejemplo de la protección de COMODO



Ejemplo de la protección de Antihook

SUPERADO EL ESCEPTICISMO QUE MARCARON LOS IDS, Y TENIENDO EN CUENTA LA MAYOR COMPLEJIDAD EN LAS COMUNICACIONES, ACTUALMENTE SE TIENDE A LA NECESIDAD DE PROPORCIONAR GESTIONES MUCHO MÁS POTENTES PARA TODOS LOS SISTEMAS DE INFORMACIÓN CON PLATAFORMAS DE HARDWARE DE MAYOR CAPACIDAD.

aplicativos vulnerables ya que existen muchos servidores con sistemas operativos que no pueden mantenerse actualizados constantemente. Los sistemas IPS pueden detectar una intrusión gracias al trabajo conjunto con otras herramientas de seguridad.

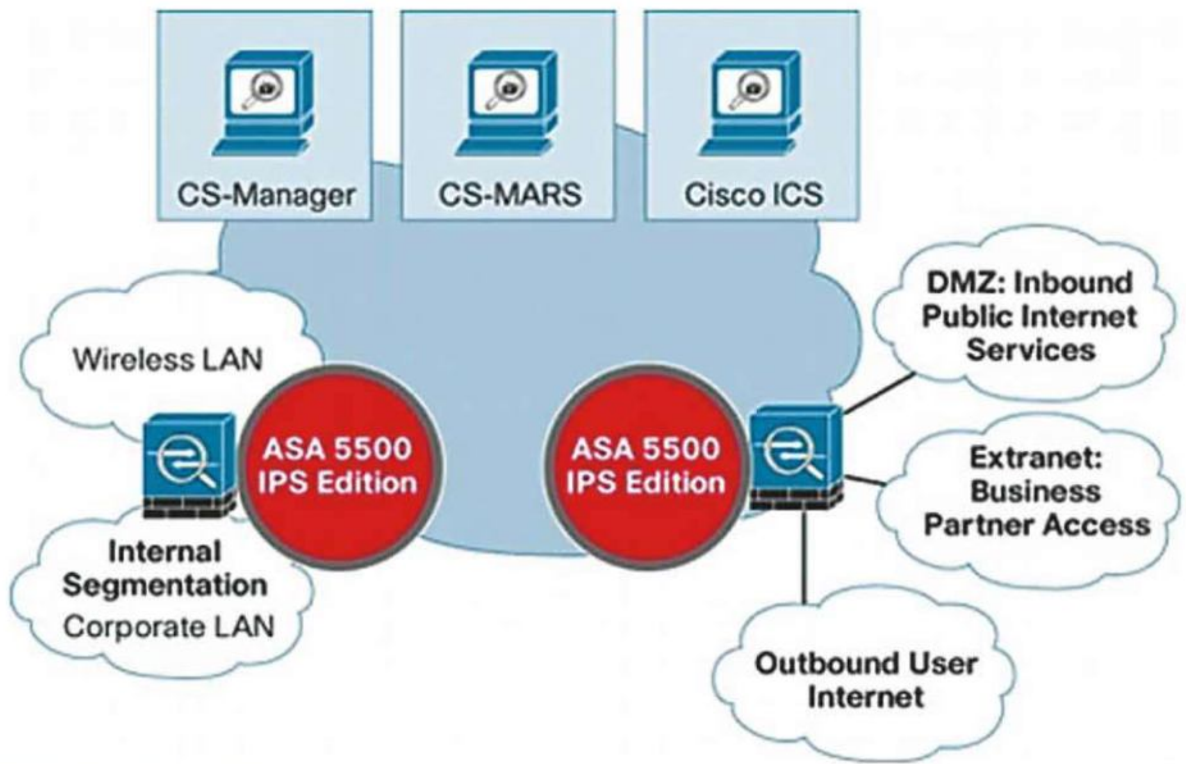
Sin embargo, la principal virtud de los IPS no está ni en la protección del tráfico interno ni de los aplicativos vulnerables, sino en la visión global de seguridad sobre el tráfico de la red que aportan, proporcionando información sobre los protocolos que dejan pasar los cortafuegos, el tráfico que envían los PCs de un departamento contra los servidores, el flujo que consume el ancho de banda o sobre si se están cumpliendo las políticas de uso de red de la compañía.



Ejemplo de la protección de Kaspersky

Enorme potencial

Tras la decepción provocada por los sistemas IDS, la implantación de los IPS no ha sido fácil. Responsables del sector reconocen que tratar de mostrar a las compañías el enorme potencial de estas soluciones ha sido una tarea dura. Aún así, los resultados de los últimos dos años hablan de un despunte en proyectos e instalaciones ya que este segmento crece más del 20% anual a nivel global, un incremento en parte debido a que organizaciones estatales, com-



Arquitectura de la solución 5500 de Cisco



pañías financieras y telecos necesitan de estas herramientas para mantener libre de peligro la ingente cantidad de datos que manejan. Un cambio de discurso en la presentación de estas soluciones, mucho más práctico, podría explicar la explosión de este mercado. El cliente valora el mensaje acerca de qué le aportaría un sistema IPS en su caso particular, y ese conocimiento y valoración positiva de tales herramientas afianza la tendencia de crecimiento.

Los ataques llegan igual a una empresa de 10 empleados como de 10.000 y, al fin y al cabo, los sistemas de prevención no son más que instrumentos que garantizan la seguridad en las comunicaciones. Pero aunque la protección que se le debe ofrecer a una gran compañía debe ser igual a la que se le ofrezca a una pyme, siempre y cuando su negocio así lo requiera, las herramientas IPS no han conseguido por el momento adaptarse plenamente a empresas pequeñas en términos de costes.

Pero esa barrera psicológica del precio no es el único reto que deben afrontar las soluciones de prevención. Además de adaptar los costes al tamaño de la empresa, también es importante diseñar unos servicios lo suficientemente atractivos que respondan a sus necesidades.

Así las cosas, se abre la posibilidad de contratar un servicio de seguridad del mismo modo que se contrata una línea de teléfono o una conexión a Internet y entran en juego conceptos como seguridad gestionada, outsourcing, niveles de servicio garantizados... que tengan una mayor justificación para el cliente desde el punto de vista económico. La pelota está en el tejado del proveedor, que tendrá que proponer paquetes estandarizados y soluciones llave en mano para las pymes.

Tendencias de futuro

Superado el escepticismo que marcaron los IDS, y teniendo en cuenta la mayor complejidad en las comunicaciones, actualmente se tiende a la necesidad de proporcionar gestiones mucho más potentes para todos los sistemas de información con plataformas de hardware de mayor capacidad.

El futuro de los IPS se centra en la mayor integración en cualquier dispositivo que forme parte de una red y en ofrecer una visión de seguridad global, unificada y constituida por elementos que interaccionen unos con otros, que se comuniquen, y no por mecanismos aislados en los que cada parte proporcione unos volúmenes de información incapaces de descifrar y analizar a no ser que se posea una elevada cantidad de efectivos dedicada a estas tareas.

Los expertos apuntan que la próxima generación de sistemas de seguridad perimetral integrará su capacidad con la de un IPS, colaborarán entre sí a la hora de tomar decisiones, huyendo de los análisis desde perspectivas separadas. Se vislumbra, por tanto, un futuro prometedor en los sistemas integrados y de servicios ya que la tecnología IPS se está convirtiendo cada vez más en un componente clave en la protección de las empresas y será incluso más importante para las compañías en el futuro, ya sean proveedores de servicios, organismos gubernamentales, telecos o cualquier otra corporación. Por tanto, el uso de los IPS se ha generalizado de tal manera que son pocos los fabricantes que no lo incluyen en sus productos y, a fecha de hoy, resulta la alternativa más eficiente frente a otras soluciones de seguridad del mercado.

En el mundo de la movilidad, el trabajo con grandes cantidades de tráfico ha obligado a cambiar el concepto de seguridad en las redes. Tratar tanto volumen de información de fuentes muy dispersas resulta complicado y aquí es donde los sistemas de prevención de intrusos van a tener un papel conciliador.

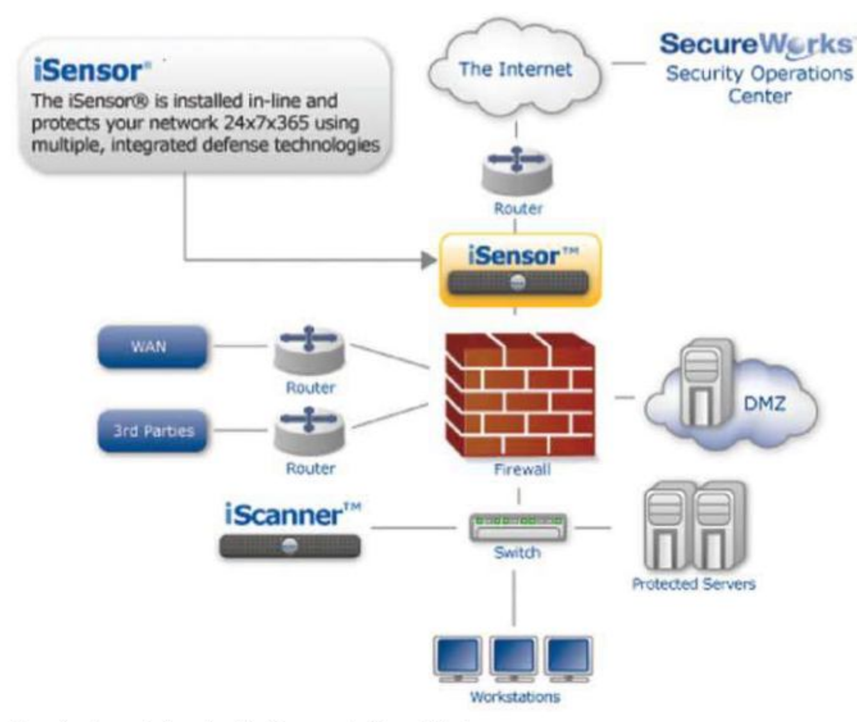
Cada una de las herramientas informáticas desempeña su rol, pero la mayoría de ellas genera una serie de registros de lo que está ocurriendo en la red. Los IPS recogen los datos que llegan de cortafuegos, servidores y otros focos y proporcionan respuestas integradas sobre lo que está pasando en las redes, tanto los intentos de ataque, o malware, como la manera de solucionar problemas detectados. Actúan, por tanto, de manera proactiva e integradora: ahí está la clave de su éxito en un ambiente en el que la seguridad resulta básica para hacer frente a un número cada vez mayor de ataques.

>>> TIPOLOGÍA DE IPS

Un IPS puede definirse como un dispositivo que tiene la capacidad para detectar amenazas, tanto conocidas como desconocidas, previniendo que el ataque se lleve a cabo. Existen dos estándares básicos de IPS:

- **NIPS: sistemas basados en red. Plataforma independiente que identifica intrusiones examinando el tráfico de red y monitorizando múltiples host de dicha red a la que protege.**
- **HIPS: sistemas basados en host. Consiste en un agente o programa instalado en un host que identifica intrusiones en dicha máquina analizando diferentes actividades. Ejercen su protección frente a máquinas individuales y son los más utilizados en la actualidad para la defensa de los entornos corporativos.**

LA PRINCIPAL VIRTUD DE LOS IPS NO ESTÁ NI EN LA PROTECCIÓN DEL TRÁFICO INTERNO NI DE LOS APLICATIVOS VULNERABLES, SINO EN LA VISIÓN GLOBAL DE SEGURIDAD SOBRE EL TRÁFICO DE LA RED QUE APORTAN.



Arquitectura de la solución iSensor de SecueWorks

WATCHMEN









Dos juegos en uno

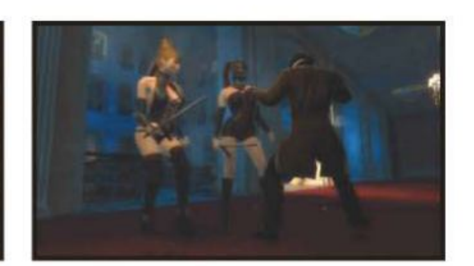
WATCHMEN: El fin está cerca consta de dos partes en un solo videojuego para adultos, presentado en julio de este año y basado en la obra de Warner Bros Pictures del mismo nombre dirigida por Alan Moore y Dave Gibbons. Es único para Xbox 360, Playstation 3 y PC en 2009.

Una de sus principales novedades se encuentra en la posibilidad de elegir entre un modo cooperativo de pantalla dividida o un modo individual con un compañero controlado por inteligencia artificial. Por tanto, el jugador puede introducirse en la piel de dos de los protagonistas, Rorschach o Nite Owl, pudiendo jugar tanto solo como acompañado.

La primera parte cuenta la historia del origen de estos dos superhéroes enmarcada una década antes de la historia que se desarrolla en la película. En la segunda, Rorschach contacta con Nite Owl y ambos vuelven a formar un equipo para resolver el caso de una chica desaparecida, Violet Greene. En su camino descubrirán que una mujer de su pasado forma parte de la trama de la desaparición creando un conflicto de intereses entre ambos héroes enmascarados. El jugador se sentirá realmente como uno de los protagonistas ya que Patrick Wilson y Jackie Earle Haley, los actores que encarnan a estos personajes, han realizado el doblaje de las voces en el videojuego.

Los protagonistas lucharán en diferentes batallas sangrientas en las que demuestran sus habilidades para el combate y cuenta con una colección de golpes finales que hará las delicias del usuario. En cada capítulo se puede luchar contra veinte enemigos a la vez en peleas callejeras brutales. Todas sus pantallas están elaborados a base de los acontecimientos de la película y, además, los escenarios son fieles a los de la misma cuidando hasta el último detalle.



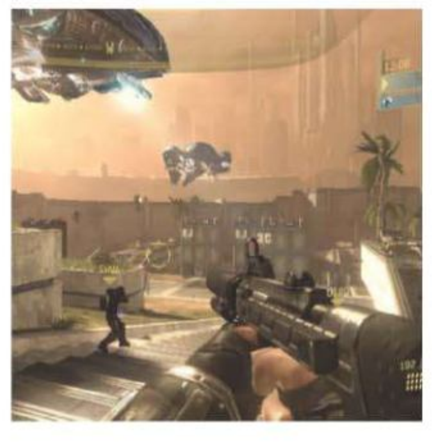


HALO 3 ODST

Acción, tiros y estrategia

Una de las sagas de ciencia ficción más importantes del mundo de los videojuegos tendrá en las tiendas una nueva versión a partir del 22 de septiembre para la consola Xbox 360. Halo 3: ODST pondrá al jugador en la piel de un soldado encargado de localizar un escuadrón perdido y averiguar los motivos de la invasión de Nueva Mombasa a cargo de los Convenant.

Desde que hace tres años Bungie Studios lanzara Halo 3, se esperaba con expectación la llegada de una nueva aventura. La cuestión es si este videojuego logrará alcanzar la cota de éxito de sus predecesores: más de 25 millones de personas en todo el mundo desde 2001 ha disfrutado alguna vez del divertimento y emoción que garantiza esta saga. Con estos antecedentes, ¿qué prestaciones ofrece para satisfacer a sus muchos seguidores e incluso para enganchar a otros nuevos? Empezando por un tipo de acción que se acerca ligeramente a la aventura gráfica y un motor multijugador que hará las delicias de los jugadores on-line, todo son buenas noticias.



Esta entrega abre una nueva perspectiva dentro del universo Halo. Cronológicamente se sitúa entre el Halo 2 y el Halo 3 y el protagonista ya no será el Jefe Maestro, el único personaje de videojuego que tiene una figura en el museo Madame Thoussaud de Londres. Ahora, el papel principal lo encarna un soldado que deberá reunir pistas a la vez que elimina a los numerosos enemigos que se interpondrán en su camino. Entre sus debilidades se encontrará su vulnerabilidad: ya no es un ser casi sobrenatural como el anterior protagonista de la saga, sino un hombre que no tiene capacidad casi ilimitada para sobrevivir a las balas y los ataques. Por ello, se deberá tener más cuidado cuando se enfrente a los enemigos. Pero como no todos son des-



ventajas a la hora de encarnar a un marine, esta vez el personaje tiene compañeros que ayudarán a salir mejor parado de las situaciones complicadas. Además, cuando de junte con ellos, el jugador cambiará de rol y, de manera retrospectiva, se convertirá en uno de los soldados desaparecidos que los personajes de Halo 3:ODST tratan de encontrar.

El armamento que utilizará es distinto. Para compensar su vulnerabilidad, tendrá radares para localizar los peligros, casco con visor nocturno y estará capacitado para atacar a los Convenant con armas silenciosas. Ello da fe de hasta que punto este videojuego trata de ir más allá de ser un mero shooter, contando con una importancia primordial la estrategia. Los marines, orquestando juntos, pueden asaltar a sus enemigos por sorpresa y sin hacer un gran ruido que provoque que más monstruos acudan en su ayuda. No sólo habrá que ser rápido, sino que también será necesario utilizar la inteligencia.

Otra de las novedades son los escenarios que incluye. Ya no se trata de ir atravesando pantallas, sino que todo el videojuego se desarrolla en una localización completamente abierta a la exploración y que hace posible que el usuario elija en todo momento a donde debe dirigirse.

¿Y que hay del módulo de multijugador? Utilizándolo, el jugador formará parte de un equipo de cuatro personas que se necesitarán mutuamente para poder sobrevivir. Se trata sin duda de una de las grandes novedades de este juego que, pese a que se trató de incluir en el Halo 3, finalmente se quedó en la mesa de operaciones. El equipo tendrá un número de vidas determinado para todo el grupo y un tiempo límite. Los enemigos a los que se enfrentarán son los mismos que en el juego normal, si bien las localizaciones son distintas e incluirán mapas para poder orientarse mejor por ellas. Adicionalmente a todo ello, al adquirir Halo 3:ODST, se podrá disfrutar de un pequeño adelanto de Halo Reach, la nueva entrega del juego que no llegará hasta 2010.





Que la fuerza te acompañe

A muchos no les cae bien el rancio de Luke Skaywalker. Siendo conscientes de ello, la factoría LucasArts lanzó en septiembre de 2008 "El poder de la fuerza", un videojuego en el que el usuario se une al bando de los malos. Este otoño se pondrá a disposición de los numerosos seguidores de la saga la primera de sus extensiones. La historia comienza con el personaje ocupando un lugar de privilegio a la derecha del Emperador. Darth Vader ha muerto y ahora el poder del mal está en sus manos, siendo el lord Sith más poderoso del universo. Su misión será la de volar hasta el planeta Tatooine para eliminar a Obi-Wan Kenobi, que está escondido en él como se cuenta en la película La venganza de los Sith. Mientras busca en solitario al Jedi, se encontrará con otros personajes de la saga como Jabba el Hutt o el cazarecompensas Boba Fett.

Para hacerse con este videojuego, habrá que descargarlo directamente desde Xbox 360 de Microsoft y Playstation 3. Y para los más acérrimos del juego, a finales de año LucasArts planea sacar también para Xbox 360 y Playstation 3 "El poder de la fuerza: Edición Sith", que añade al juego original tres nuevos niveles para originar una variante maligna a lo que sucede en las películas de las dos trilogías cinematográficas. El usuario podrá realizar misiones en Tatooine o Hoth, el planeta helado donde se desarrolla el comienzo de El imperio contrataca. Allí deberá aplastar una rebelión liderada nada y más nada menos que por Luke Skaywalker.







Gestionar a distancia un ordenador

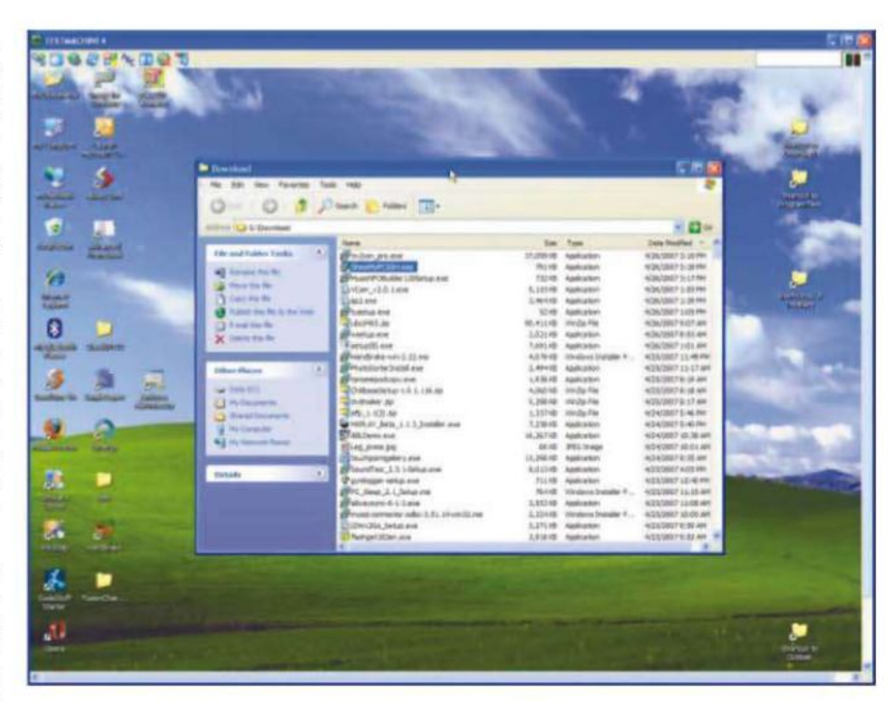
Manejar un ordenador remotamente desde otro equipo se esté donde se esté es posible con el programa ShowMyPC que, además, funciona tanto en un PC Windows como en un Mac. Basta con una llave USB y una serie de sencillas instrucciones.

Cuando se está fuera de la oficina o de casa, controlar el ordenador remotamente era hasta hace poco una tarea casi imposible. De aquí a un tiempo, sin embargo, existen en el mercado varias aplicaciones que acercan esta posibilidad a los usuarios. Es el caso de ShowMyPC, una herramienta que hace posible manejar los programas de otro equipo o a distancia, e incluso, transferir sus archivos a otros puntos en los que sean necesarios.

Obtener este programa es muy sencillo: se descarga fácilmente desde la web http://showmypc.com. Una vez hecho esto, aparecerá en la pantalla del equipo el icono de la aplicación que podrá guardarse en una llave para tenerlo listo para usar desde otro dispositivo. Antes, sin embargo, habrá que iniciarlo en este PC. Se pulsa sobre el icono y a los pocos segundos aparecerá en la esquina inferior izquierda una clave que será necesario apuntar.

Se va posteriormente al equipo desde el que se quiere controlar a remoto el primer sistema y se introduce la memoria USB. Se inicia la aplicación y surgirá una ventana en la que habrá que pulsar el botón Ver un PC Remoto. Se introduce la contraseña que se obtuvo anteriormente y, automáticamente, se establecerá conexión apareciendo la pantalla del primer ordenador y pudiendo trabajar en ella con normalidad.

Pero esta aplicación también puede utilizarse en equipos Mac. Para ello hay que realizar una invitación desde programa ShowMyPC instalado en la primera computadora, y enviarla a una dirección de correo electrónico. El receptor deberá hacer click sobre un enlace en la parte de abajo del mail en el que pone http://assured.showmypc.com/mac/index.html. Se establecerá una conexión automática con el programa y, una vez se introduzca la clave, el ordenador remoto tendrá en la venta el escritorio al que se ha accedido de manera remota, pudiendo manejarlo como si estuviera presente.







Filtrar e-mails con mayor seguridad

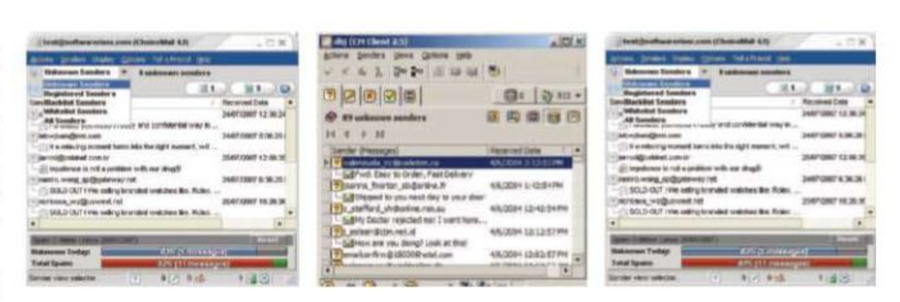
Hoy en día la mayoría de cuentas de correo electrónico poseen un filtro antispam con el que eliminar cualquier mensaje no deseado. Si aún así queremos seleccionarlos para filtrarlos con mucha más confianza una aplicación muy útil es ChoiceMail One.

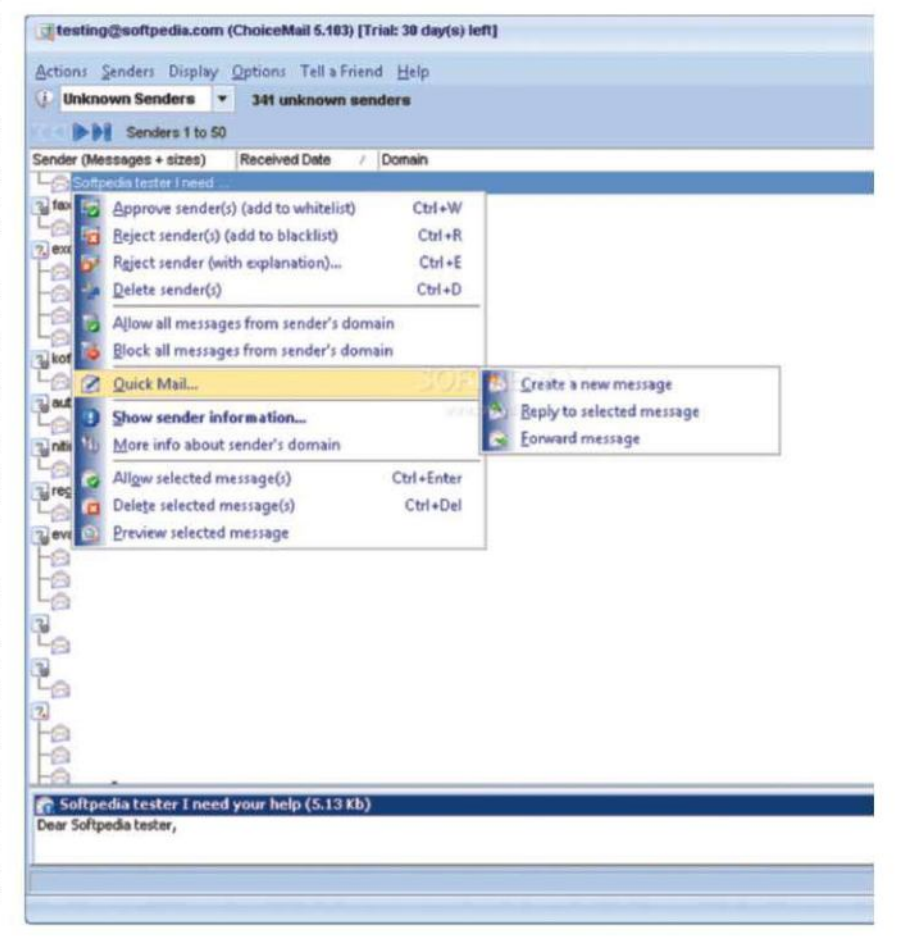
Lo primero que hay que hacer es descargarse este programa desde www.digital-portal.com. Una vez instalado, se utiliza el campo Destination Folder para seleccionar la carpeta de instalación de los archivos del programa. El acceso directo aparecerá en el escritorio pero, como es la primera vez que se inicia, aparece un aviso de configuración.

Antes de continuar se tiene que cerrar el correo electrónico. Posteriormente, en un recuadro se verán las opciones de correo con el que se quiere que trabaje ChoiceMail. La aplicación detectará automáticamente las cuentas configuradas, cuando aparezcan se seleccionará la elegida para el filtrado. Para terminar la configuración de la cuenta se escribe la información de la misma, el nombre del usuario y la contraseña. Una vez hecho esto, la aplicación ya está configurada y lista para usarse.

Al comienzo, un recuadro sugiere que se deberían importar los datos de los contactos del correo. Esto es así porque todos los mensajes del programa se aceptarán automáticamente. Una vez realizada esta acción, los mensaje se pueden proteger seleccionando en el menú la opción Actions y después Check for New Mail. Los mails irán saliendo en la ventana principal y se puede hacer un seguimiento de la descarga en la esquina inferior derecha.

En caso de que algún correo electrónico recibido sea un emisor conocido pero el programa lo marque como que no lo es, pinchando sobre él con el botón derecho del ratón y seleccionando Aprobé sender(s) (add to whitelist), su dirección pasará a formar parte de las direcciones aceptadas. Por el contrario, si alguno no deseado ha pasado el filtro, lo que hay que hacer es pinchar también el botón derecho del ratón para elegir la opción Reject sender (with explanation) para que el emisor pase a la lista negra y no se vuelva a recibir e- mails de esa dirección.





Zona móviles

PANDAMANÍA+CROSSPIX, PUZZLES PARA EJERCITAR LA MENTE

Para afinar las habilidades y desafiar al cerebro con una diversión adictiva, nada mejor que disfrutar de estos dos juegos desarrollados por Glu Mobile en la pantalla del teléfono. Pandamanía presenta al usuario una tarea simple: guiar a un oso para que aliené tres o más bolas del mismo color y hacerlas así explotar. Cuantas más pelotas se revienten, más puntos se obtendrán. Por su parte, CrossPix dispone de muchas imágenes de gran resolución que hacen posible configurar una colección de cuadros muy amplia, no sin antes colocarlos de manera correcta requiriéndose para ello el ingenio y la rapidez mental.







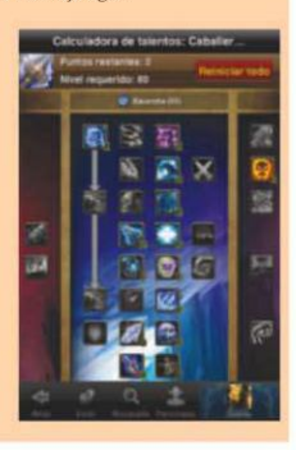


ARMERÍA MÓVIL DE WORLD OF WARCRAFT

Esta aplicación para el iPhone se dirige a aquellos que sean usuarios y tengan una cuenta en el juego en Red World of Warecraft,. En ella, se puede hacer lo mismo que en la página web de la Armería (eu.wowarmony.com): encontrar todos los personajes de World of Warcraft junto a su equipo, atributos y logros; acceder a estadísticas de hermandad, calendario de juego y tabla de líderes; y usar la calculadora de talentos para decidir la mejor distribución para el personaje e informarse de las últimas noticias del videojuego.







SONIC JUMP+ENTRENA TU MENTE



Para estimular la mente y, a la vez, pasar un buen rato, estos dos juegos se combinan a la perfección. Entrena tu mente propone una serie de actividades y puzzles acompañados de ejercicios desafiantes de sudoku. Incluye gráficos para que el usuario vea sus evoluciones. Y para descargar adrenalina, nada mejor que vivir aventuras con el erizo más famoso de la historia: Sonic. Esta vez el animal se mueve también en vertical, escalando obstáculos para arruinar los diabólicos planes del doctor Robotnik. Por el camino, deberá recoger anillos que le otorguen más poder.





